Lantech

LES-2400-RPS

3-slot Modularized Fast Ethernet L2 + 2 Gigabit Copper / Mini-GBIC Combo Managed Switch

User Manual

v1.2

Apr-2011

Contents

1. INTRODUCTION 1

Features 1
Software Features 2
Package Contents 5
Ethernet Switching Technology 6

2. HARDWARE DESCRIPTION 7

Physical Dimensions 7
Front Panel 7
LED Indicators 8
Rear Panel 9
Desktop Installation 10
Rack-mounted Installation 10
Power On 12
Redundant power 12

3. NETWORK APPLICATION 13

Connecting to the Switch 14

4. CONSOLE MANAGEMENT 15

Login in the Console Interface 15
Module Hot-Swapping 16

5. WEB-BASED MANAGEMENT 17

About Web-based Management 17
Preparing for Web Management 17
System Login 18
Main interface 19
Main interface 19
System Information 20
IP Configuration 21

DHCP Server 23
TFTP 27
System Event Log 30
SNTP Configuration 36
IP Security 40
User Authentication 42
Advanced Configuration 43
Port Statistics 45
Port Control 46
Port Trunk 48
Port Mirroring 52
Rate Limiting 53
VLAN Configuration 54
Rapid Spanning Tree 62
Pro-Ring System 66
SNMP Configuration 68
QoS Configuration 74
IGMP Configuration 76
LLDP 78
802.1x/Radius 79
MAC Address Table 82
Access Control List 86
Factory Default 88
Save Configuration 89
System Reboot 90

6. TROUBLESHOOTING 91

Incorrect Connections 91
Diagnosing LED Indicators 92

7. TECHNICAL SPECIFICATIONS 93

1. Introduction

The 3-slot Modularized Fast Ethernet L2 plus + 2 Gigabit Copper / Mini-GBIC Combo Managed Switch is a modular Ethernet switch that can be used to build high-performance switched workgroup networks. This switch is a store-and-forward device that offers low latency for high-speed networking. The Switch is targeted at workgroup, department or backbone computing environments.

The 3-slot Modularized Fast Ethernet L2 plus + 2 Gigabit Copper / Mini-GBIC Combo Managed Switch features a “store-and-forward” switching scheme. This allows the switch to auto-learn and store source address in an 8K-entry MAC address table.

MDI (Medium Dependent Interface) Port is also called an "uplink port". The MDI port does not cross transmitting and receiving lines, which is done by the regular ports (MDI**-X** ports) that connect to end stations. In general, **MDI** means connecting to another Hub or Switch while **MDIX** means connecting to a workstation or PC. Therefore, **Auto MDI/MDIX** means you can connect to another Switch or workstation without changing non-crossover or crossover cabling.

The 3-slot Modularized Fast Ethernet L2 plus + 2 Gigabit Copper / Mini-GBIC Combo Managed Switch has 3 module slots. Users can purchase the modules on demand, increasing elasticity of network application.

Features

- Conforms to IEEE802.3 10BASE-T, 802.3u 100BASE-TX/FX, 802.3ab 1000BASE-T, 802.3z Gigabit SX/LX
- 3 slots for 8 ports 10/100TX, 8 ports 100Mbps multi mode fiber module, 8 ports 100Mbps single mode fiber module, or 8 ports 100Mbps SFP module
- IEEE802.3x Flow control
  - Flow control for full duplex

- Backpressure for half duplex

- High back-plane bandwidth 8.8Gbps
- Supports IEEE802.3ad Port trunk with LACP
- Broadcast storm filter supported
- IGMP supports for Multi Media application
- Supports IEEE 802.1p class of service
- Port security supported
- Port bandwidth control supported
- Supports IEEE 802.1d Spanning tree protocol
- Supports GVRP function
- Port Base VLAN/802.1Q VLAN supported
- IEEE 802.1X user authentication
- Supports DHCP client
- Web/ SNMP / Telnet / CLI management
- Optional Module for slot:
  - 8 ports 10/100TX module
  - 8 ports 100FX single mode module
  - 8 ports 100FX multi mode module
  - 8 ports 100SFP module

Software Features

Management	SNMP v1/v2c/v3, Web, Telnet, CLI, RMON1
Software Upgrade	TFTP and Console firmware upgradeable
MIB	RFC 3418 SNMP MIB RFC 1213 MIBII RFC 2011 MIB RFC 1493 Bridge MIB RFC 2674 VLAN

	RFC 1215 Trap MIB RFC 1643 Ethernet like RMON1 Private MIB
SNMP Trap	Cold/warm start trap, link down/link up trap, authorization fail trap, fan fail trap. power event trap
Port Trunk	Supports IEEE802.3ad with LACP function. Up to 13 trunk groups, trunk member up to 4 ports and include 2 uplink ports
Spanning Tree	IEEE802.1d spanning tree, IEEE 802.1w Rapid Spanning tree protocol
VLAN	Port based VLAN, up to 24 groups IEEE802.1Q Tag VLAN Static VLAN groups up to 256, Dynamic VLAN group up to 2048, VLAN ID from 1 to 4094. GVRP up to 256 groups
QOS Policy	Port based, Tag based, IPv4 Type of service, IPv4 Different service.
Class of Service	Per port 4 queues, High/ low queue. Service rule: first come first service; all High before Low, WRR for High or low weight. Weight round ratio (WRR): 8:4:2:1
IGMP	It supports IGMP V1 and V2 snooping; IGMP Snooping for Multi-Media application, IGMP group supports 256 groups and IGMP query
Port Security	Support 50 entries of MAC address for static MAC and another 50 for MAC filter
Port Mirror	Support 3 mirroring types: “RX, TX and Both packet”

Bandwidth Control	Per port support ingress rate limiting and egress rate shaping control. The rate limiting and rate shaping can be setting from 0~100Mbps
802.1x Authentication	Support IEEE802.1x User-Authentication and can report to RADIUS server. ■ Reject ■ Accept ■ Authorize ■ Disable
DHCP	DHCP Client/Server
Packet filter	Broadcast storm control

Package Contents

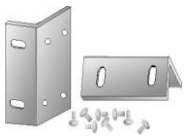
Unpack the contents of the 3-slot intelligent chassis switch and verify them against the checklist below.

- 3-slot intelligent chassis switch
- Power Cord
- Four Rubber Feet
- RS-232 cable
- Rack-mounted kit
- User Manual (CD-ROM)

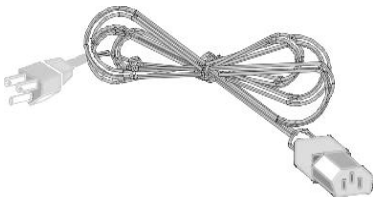
3-slot intelligent chassis switch

Four Rubber Feet

RS-232 Cable



Rack-mounted Kit



Power Cord

User Guide CD-ROM

Package Contents

Compare the contents of your 3-slot intelligent chassis switch package with the standard checklist above. IF any item is missing or damaged, please contact your local dealer for service.

Ethernet Switching Technology

Ethernet Switching Technology dramatically boosted the total bandwidth of a network, eliminated congestion problems inherent with CSMA/CD (Carrier Sense multiple access with Collision Detection) protocol, and greatly reduced unnecessary transmissions.

This revolutionized networking. First, by allowing two-way simultaneous transmissions over the same port (Full-duplex) essentially doubled the bandwidth. Second, by reducing the collision domain to a single switch-port eliminated the need for carrier sensing. Third, by using the store-and-forward technology's approach of inspecting each packet to intercept corrupt or redundant data eliminated unnecessary transmission that slow the network. By employing address learning replaced the inefficient receiving port.

Auto-negotiation regulates the speed and duplex of each port, based on the capability of both devices. Flow-control allows transmission from a 100Mbps node to a 10Mbps node without loss of data. Auto-negotiation and flow-control may require disablement for some networking operations involves legacy equipment. Disabling the auto-negotiation is accomplished by fixing the speed or duplex of a port.

Ethernet Switching Technology supplied higher performance at costs lower than other solutions. Wider bandwidth, no congestion, and the reduction in traffic is why switching is replacing expensive routers and inefficient hubs as the ultimate networking solution. Switching brought a whole new way of thinking to networking.

2. Hardware Description

This Section mainly describes the hardware of the 3-slot intelligent chassis switch, and gives a physical and functional overview of the switch.

Physical Dimensions

The 3-slot intelligent chassis switch physical dimensions are **440mm(W) x 44mm(H) x 280mm(D)**.

Front Panel

The Front Panel of the 3-slot intelligent chassis switch supports up to 4 kinds of module. Please refer to the module user guide for further information.

LED Indicators

The LED Indicators gives real-time information of systematic operation status. The following tables describe definitions for LED indicators.

LED	Status	Description
LK/ACT	Green	The port is connecting with the device.
	Blinks	The port is receiving or transmitting data.
	Off	No device attached.
FD/COL	Yellow	The port is operating in Full-duplex mode.
	Blinks	Collision of Packets occurs in the port.
	Off	In half-duplex mode
1000	Green	The port is operating at the speed of 1000Mbps
100	Green	The port is operating at the speed of 100Mbps (for RJ-45 port only)

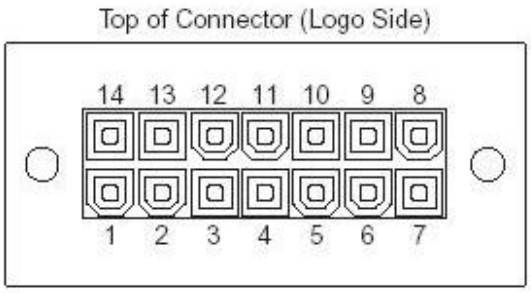
The Description of LED Indicators

Rear Panel

Equipped with a 3-pronged power plug for AC power input and a 14-pin dual-row connector for DC power input, the Ethernet switch allows users to supply AC power in the range of 100 to 240V/50-60Hz or DC power in the range of 12 to 48V for redundant supplying purposes.

The Rear Panel of the 3-slot intelligent chassis switch

Note: As the photo shown below, the DC power terminal (male) should be connected with a 2x7-pin, pitch 4.2 mm Mini Fit connector.



Pin Number	14-Pin Designation
1	GND
2	RESERVED
3	48 V
4	48 V
5	48 V
6	48 V
7	GND
8	GND
9	RESERVED
10	RESERVED
11	RESERVED
12	RESERVED
13	RESERVED
14	GND

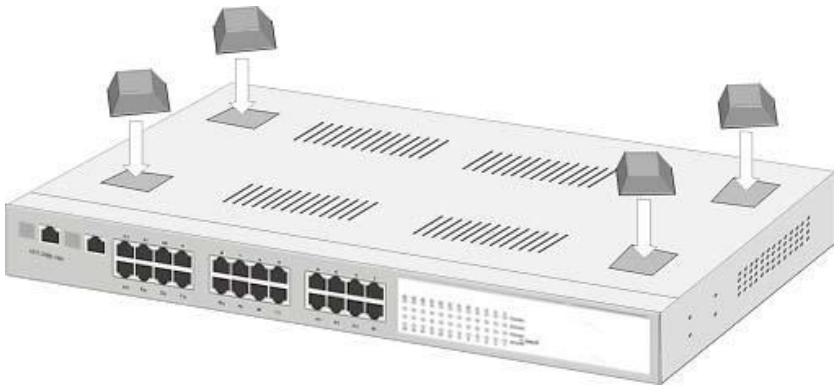
Pinouts of the DC Power Connector

Desktop Installation

Set the Switch on a sufficiently large flat space with a power outlet nearby. The surface where you put your Switch should be clean, smooth, level and sturdy. Make sure there is enough clearance around the Switch to allow attachment of cables, power cord and allow air circulation.

Attaching Rubber Feet

A. Make sure mounting surface on the bottom of the Switch is grease and dust free.
B. Remove adhesive backing from the rubber feet.
C. Apply the rubber feet to each corner on the bottom of the Switch. These footpads can prevent the Switch from shock/vibration.



Attaching rubber feet to each corner on the bottom of the Switch

Rack-mounted Installation

The 3-slot intelligent chassis switch comes with a rack-mounted kit and can be mounted in an EIA standard size, 19-inch rack. The Switch can be placed in a wiring closet with other equipment.

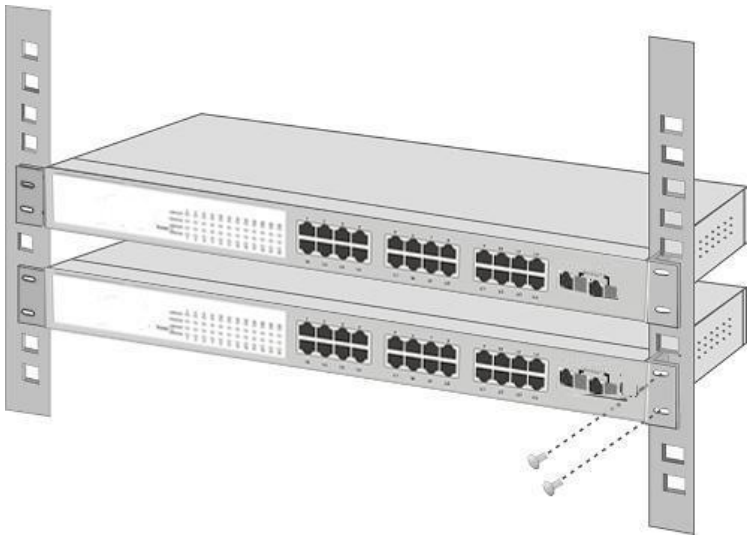
Perform the following steps to rack-mount the switch:

A. Position one bracket to align with the holes on one side of the switch and secure it

with the smaller bracket screws. Then attach the remaining bracket to the other side of the Switch.

Attach mounting brackets with screws

B. After attaching both mounting brackets, position the switch in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the Switch to the rack with a screwdriver and the rack-mounting screws.



Mount the Switch in 19” Rack

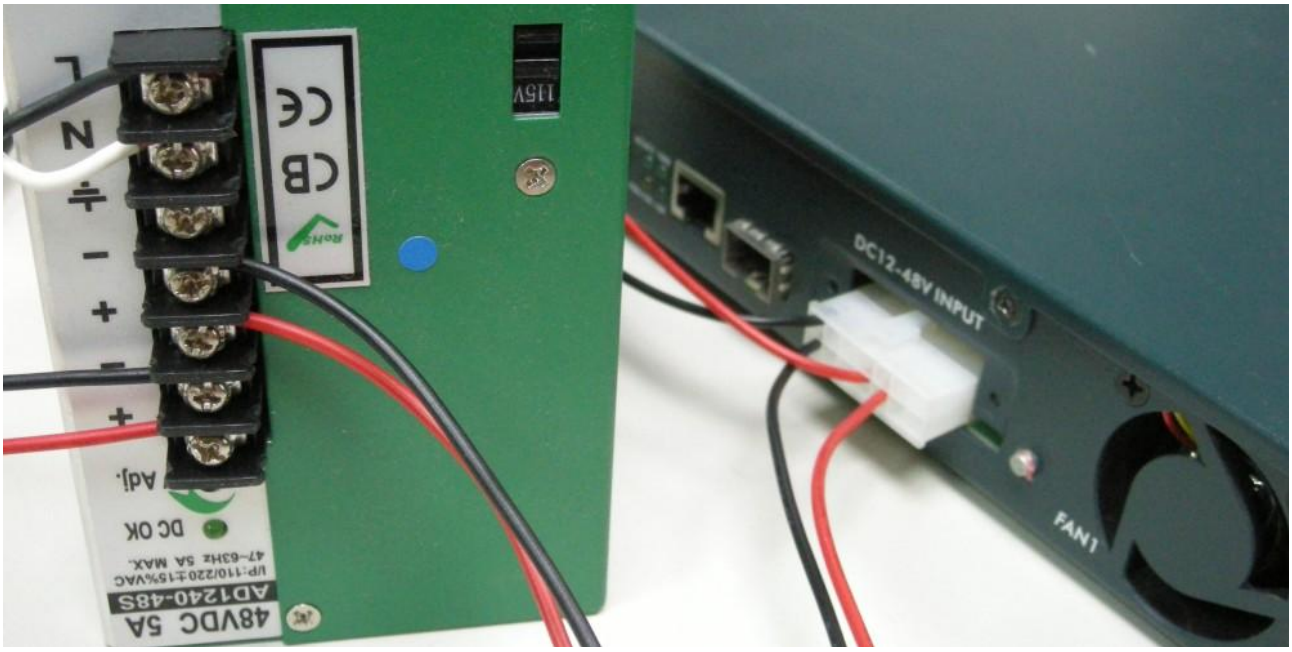
Note: For proper ventilation, allow about at least 4 inches (10 cm) of clearance on the front and 3.4 inches (8 cm) on the back of the Switch. This is especially important for enclosed rack installation.

Power On

Connect the 3-prong AC power cord or the 14-pin 2-row DC power cable to the power socket at the rear panel of the Ethernet switch. The Ethernet switch can work with AC power in the voltage range of 100-240V/50~60Hz or 12-48VDC. The AC and DC inputs can be used for redundant power supply. If one of the power inputs fails, the other one is able to keep providing power to the Ethernet switch. Check the power LED indicator on the front panel to see if power is properly supplied.

Redundant power

Connect the optional redundant power cord to the redundant power socket on the rear panel of the Switch. The other side of redundant power cord connects to the power supply. The Switch works with power supply of 12-48 VDC.



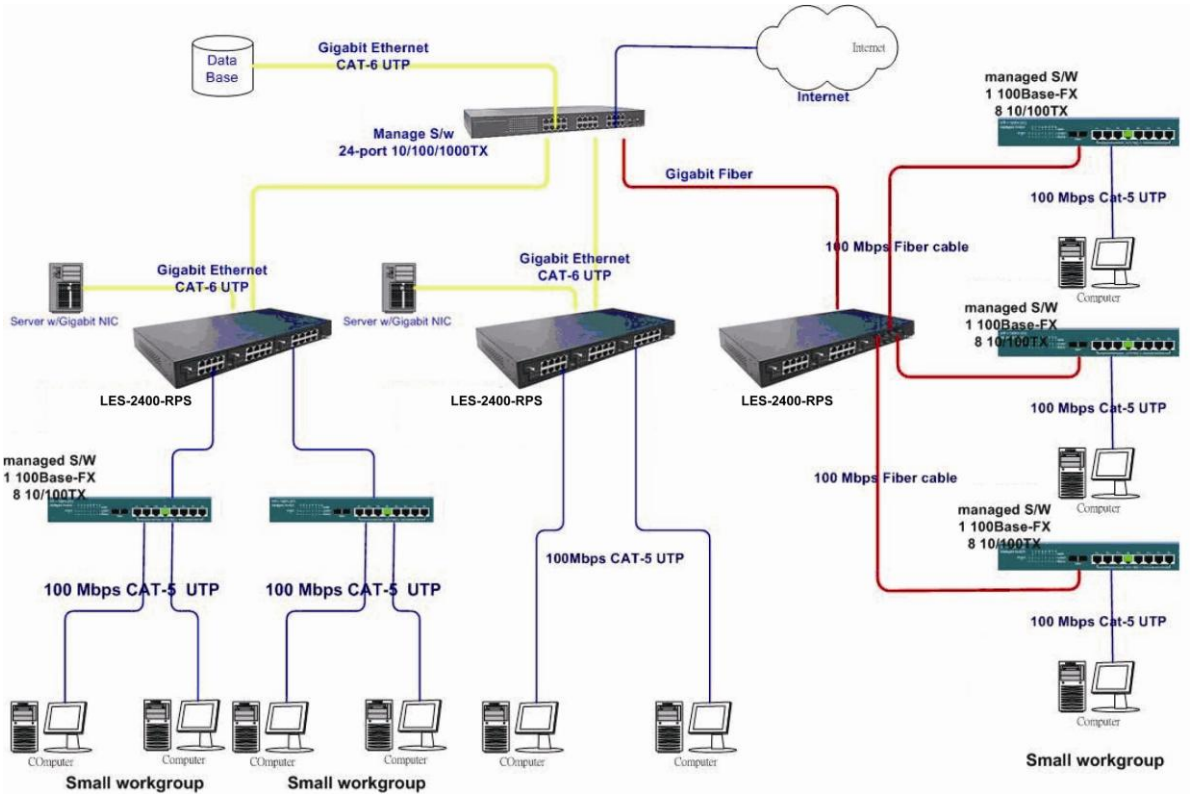
Please make sure the connection on power supply is correct when using the optional redundant power cord. Red cord should be connected to “+” and black cord should be connect to “-”.

3. Network Application

This section provides you a few samples of network topology in which the Switch is used. In general, the 3-slot intelligent chassis switch is designed as a segment switch. That is, with its large MAC address table (8K-entry) and high performance, it is ideal for interconnecting networking segments.

PCs, workstations, and servers can communicate each other via the 3-slot intelligent chassis switch. The switch automatically learns node addresses, which are subsequently used to filter and forward all traffic based on the destination address.

By using the Gigabit mini-GBIC port for long distance up-link, the switch can connect with another switch or hub to interconnect other small-switched workgroups to form a larger switched network. The figure below is an example application topology.



The example of application topology

Connecting to the Switch

The Console port is a female DB-9 connector that enables a connection to a PC or terminal for monitoring and configuring the Switch. Use the supplied RS-232 cable with a male DB-9 connector to connect a terminal or PC to the Console port.

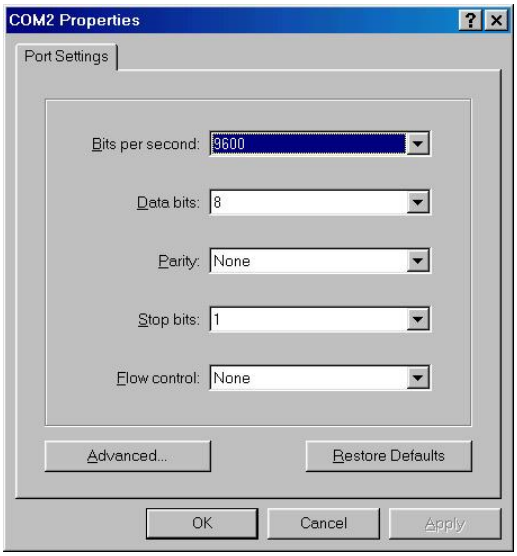
The Console configuration (out of band) allows you to set Switch for remote terminal as if the console terminal were directly connected to it.

4. Console Management

Login in the Console Interface

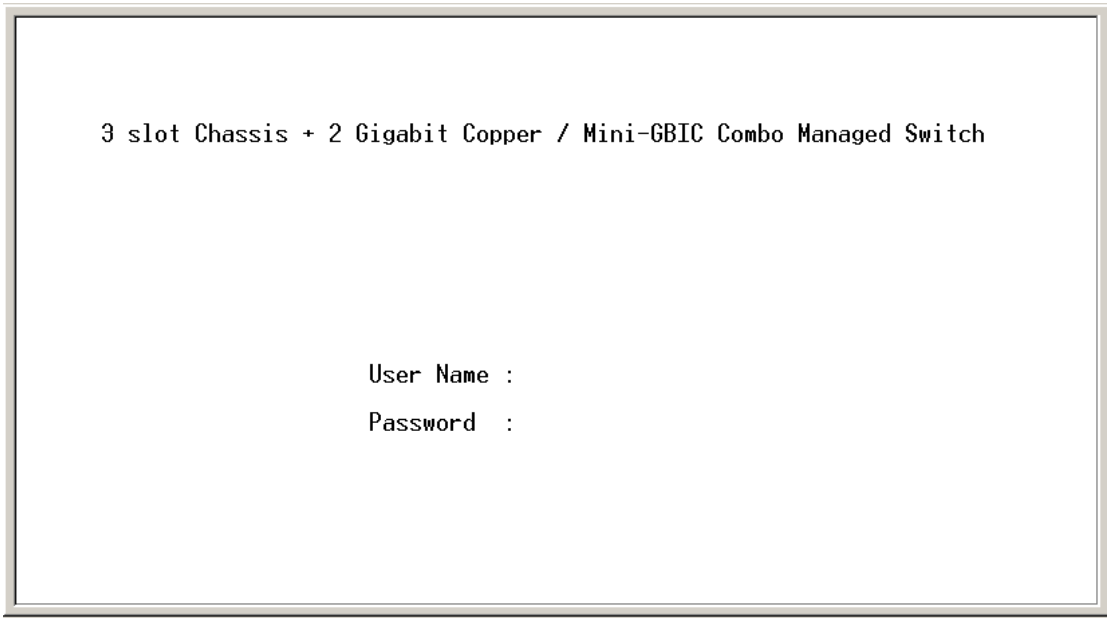
When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

Baud Rate: 9600 bps
Data Bits: 8
Parity: none
Stop Bit: 1
Control flow: None



The settings of communication parameters

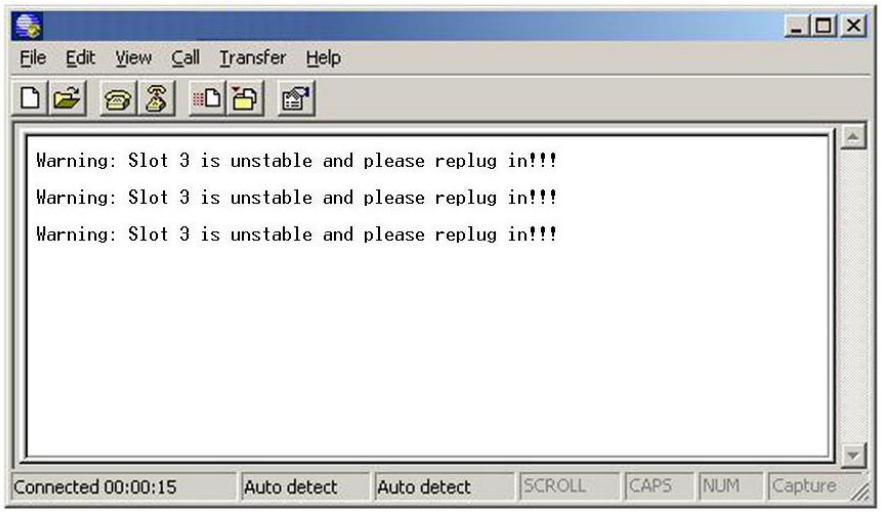
After finishing the parameter settings, click "**OK**". When the blank screen shows up, press Enter key to bring out the login prompt. Key in the "**root**"(default value) for the both User name and Password (use **Enter** key to switch), then press Enter key and the Main Menu of console management appears. Please see below figure for login screen.



Console login screen

Module Hot-Swapping

The 3-slot Modularized Fast Ethernet L2 plus + 2 Gigabit Copper / Mini-GBIC Combo Managed Switch supports module hot-swapping. User can insert or pull the module out of the slot without powering down the switch. Once the module is not fully inserted, the LEDs on the module panel will all light on at the same time. Meanwhile, the switch also sends warning message to the connected PC, work station or terminal via console port. Please see the picture as below for reference.



Warning message interface

5. Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

About Web-based Management

Inside the CPU board of the switch, there exists an embedded HTML web site residing in flash memory. It offers advanced management features and allow users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Preparing for Web Management

Before use web management, you can use console to login the switch checking the default IP of the Switch. Please refer to **Console Management** Chapter for console login. If you need change IP address in first time, you can use console mode to modify it. The default value is as below:

IP Address: **192.168.16.1**
Subnet Mask: **255.255.255.0**
Default Gateway: **192.168.16.254**
User Name: **root** Password: **root**

System Login

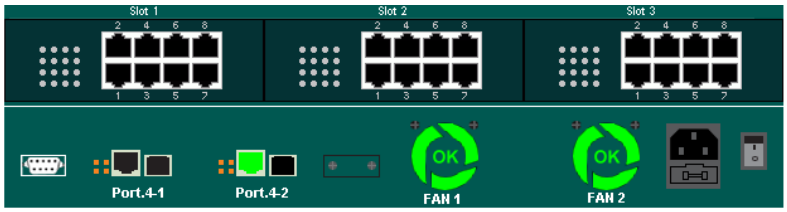
1. Launch the Internet Explorer on the PC
2. Key in “http:// “+” the IP address of the switch”, and then Press “**Enter**”.

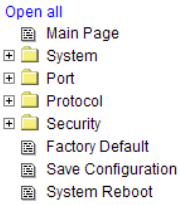
3. The login screen will appear right after
4. Key in the user name and password. The default user name and password are the same as “**root**”

Login screen

5. Press “**Enter**” key or click **OK** button, and then the home screen of the Web-based management appears as below:

Main interface





Welcome to the

3 slot Chassis + 2 Gigabit Copper / Mini-GBIC Combo Managed Switch

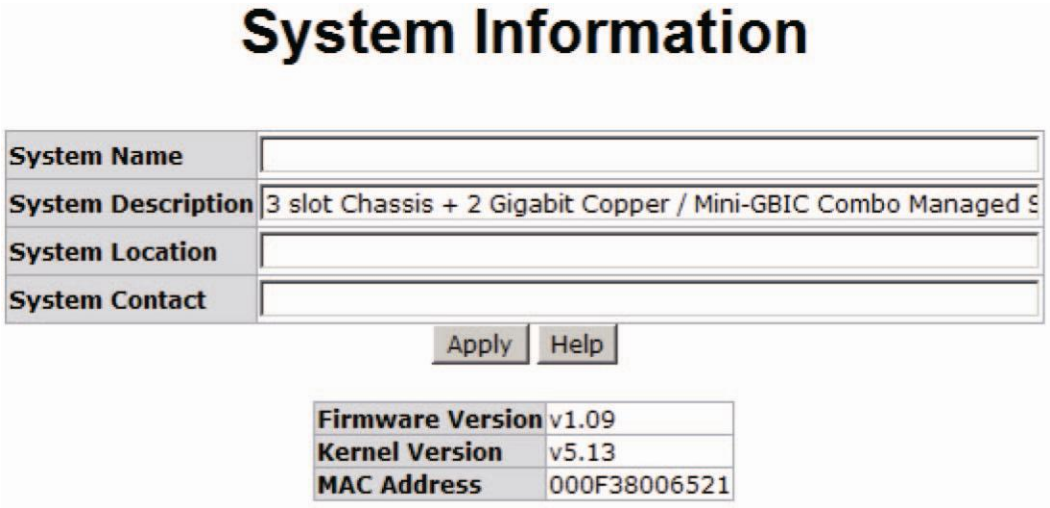
Main interface

System Information

Here you can view the system information and assign the system name and location to make this switch more easily identified on your network.

- **System Name:** Assign the name of the switch. The maximum length is 64 bytes.
- **System Description:** A read-only field displaying the description of the switch.
- **System Location:** Assign the switch physical location. The maximum length is 64 bytes.
- **System Contact:** Enter the name of contact person or department.
- **Firmware Version:** Displays the switch's firmware version.
- **Kernel Version:** Displays the kernel software version.
- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default).
- Click Apply to have the configuration take effect.

[NOTE] Don't set "0" for the first segment of the subnet mask and default gateway (000.xxx.xxx.xxx).
Refresh the web screen if the web could not be displayed while you change the setting.



System information interface

IP Configuration

- **DHCP Client**: Enable or disable the DHCP client function. When the **DHCP Client** function is enabled, the industrial switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After users click Apply, a popup dialog shows up. It is to inform the user that when the DHCP client is enabled, the current IP will lose and the user should find the new IP on the DHCP server
- **IP Address:** Assign the IP address for the industrial switch. With the **DHCP Client** function enabled, the switch is configured as a DHCP client and users doesn't need to assign the IP address that is assigned by the DHCP server. The default IP is 192.168.16.1 or the user has to assign an IP address manually when DHCP Client is disabled.
- **Subnet Mask:** Assign the subnet mask to the IP address. If the **DHCP Client** function is disabled, the user has to assign the subnet mask manually.
- **Gateway:** Assign the network gateway for the switch. If the **DHCP Client** function is disabled, the user has to assign the gateway manually. The default gateway is 192.168.16.254.
- **DNS1:** The abbreviation of Domain Name Server—an Internet service that translates domain names into IP addresses. The domain name is in alphabetic order, which is easy to be remembered. The Internet is based on IP address. Therefore, every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.net.com might translate to 192.168.16.1.
- **DNS2:** The backup for DNS1. When DNS1 cannot function, DNS2 will then replace DNS1.
- When finished, click Apply to have the configuration take effect.

IP configuration interface

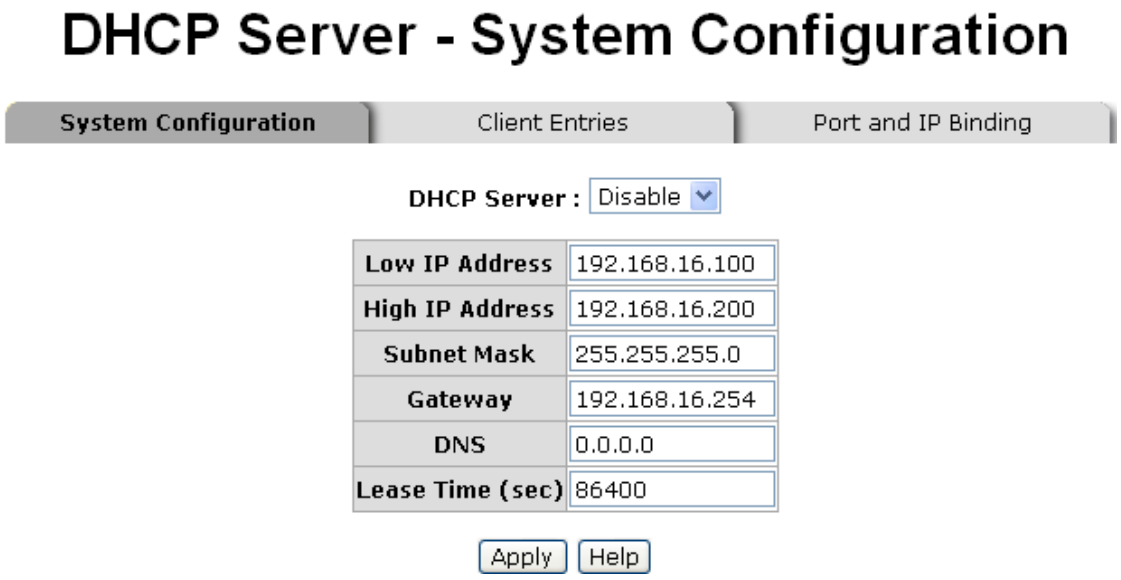
DHCP Server

DHCP is the abbreviation of Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requires an administrator to manage the task. This means that a new computer can be easily added to a network without the hassle of manually assigning it a unique IP address.

The system provides the DHCP server function. With the DHCP server function enabled, the switch system is able to be configured as a DHCP server.

System configuration

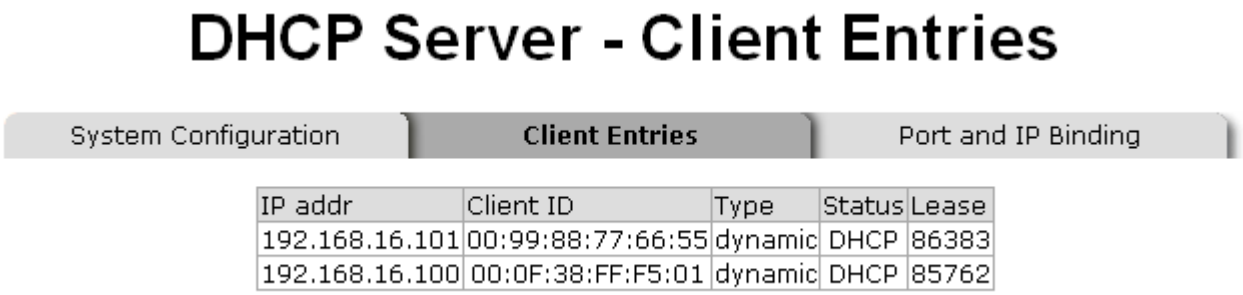
- **DHCP Server:** This pull-down menu allows you to configure the switch to be the DHCP server on your local network.
- **Low IP Address:** Type in an IP address as the beginning of a range of the dynamic IP address. As the figure shown below, for example, 192.168.16.100 is the relatively low IP address of the range.
- **High IP Address:** Type in an IP address as the beginning of a range of the dynamic IP address. As the figure shown below, for example, 192.168.16.200 is the relatively high IP address of the range.
- **Subnet Mask:** Type in the subnet mask of the IP configuration.
- **Gateway:** Type in the IP address of the gateway in your network.
- **DNS:** Type in the IP address of Domain Name Server in your network.
- **Lease Time (sec):** The length of time the dynamic IP addresses assigned to clients.
- Click Apply to have the configuration take effect.



DHCP Server Configuration interface

Client Entries

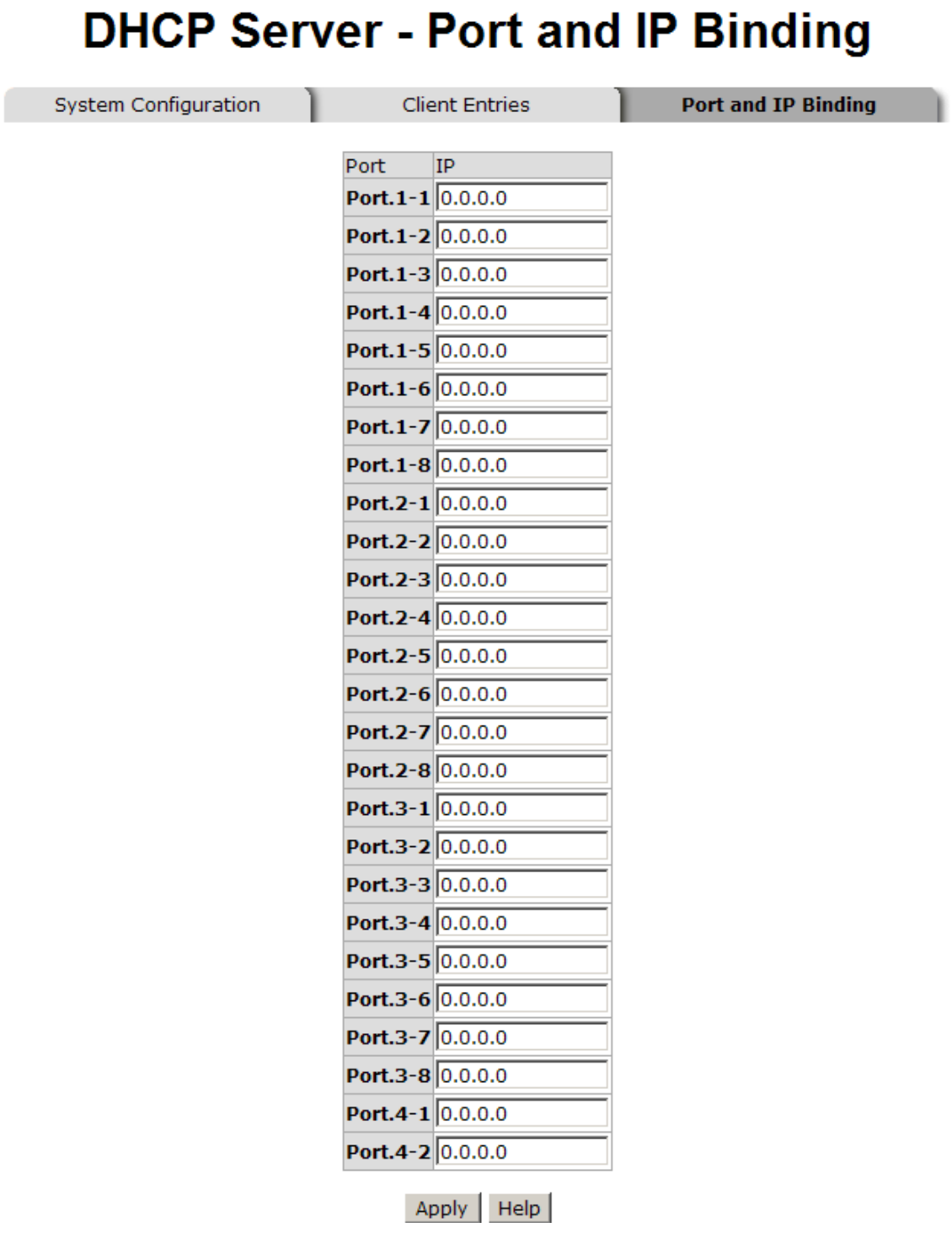
When the **DHCP Server** function is enabled, the system will collect the DHCP client information including the assigned IP address, the MAC address of the client device, the IP assigning type, states and lease time.



DHCP Client Entries interface

Port and IP Bindings

As the figure shown below, the switch will assign the IP address to the connected client according to the Port-IP binding table. The user is allowed to fill each port with one particular IP address. When the device is connecting to the port and asks for IP assigning, the system will assign the IP address bound with the port to the device.



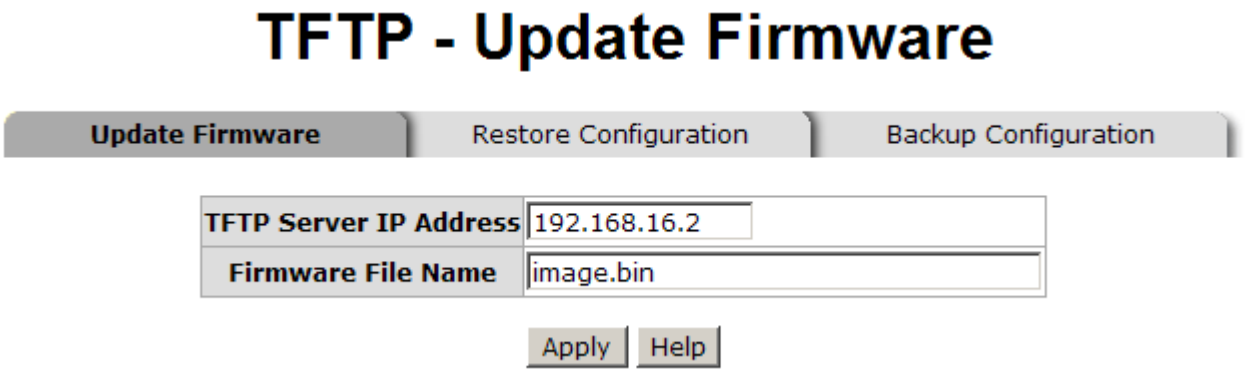
Port and IP Bindings interface

TFTP

It provides the functions allowing the user to update the switch firmware via the Trivial File Transfer Protocol (TFTP) server. Before updating, make sure the TFTP server is ready and the firmware image is located on the TFTP server.

Update Firmware

- **TFTP Server IP Address:** Type in the IP address of the TFTP server.
- **Firmware File Name:** Type in the name of the firmware image file to be updated.
- When finished, click Apply to start updating.

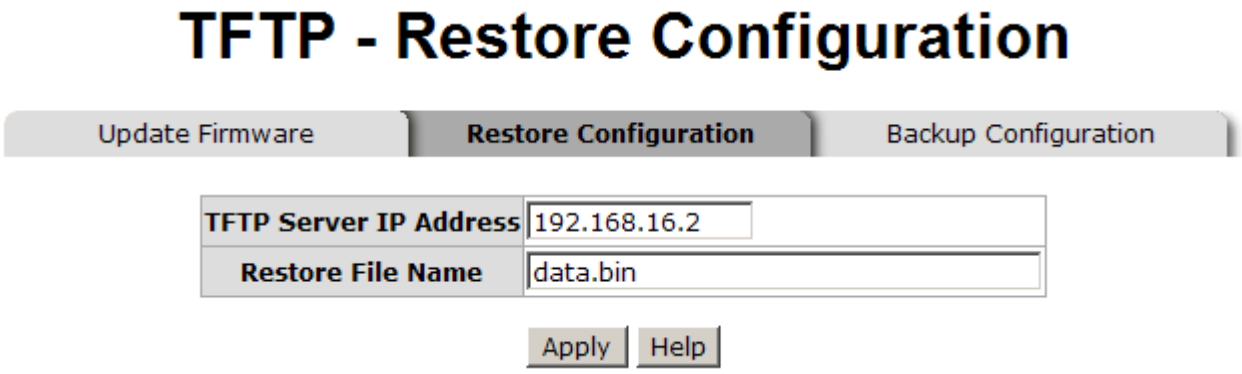


Update Firmware interface

Restore Configuration

You can restore a previous backup configuration from the TFTP server to recover the settings. Before doing that, you must locate the image file on the TFTP server first for the switch to download back the flash image.

- **TFTP Server IP Address:** Type in the IP address of the TFTP server.
- **Restore File Name:** Type in the correct file name for restoring.
- When finished, click Apply to start configuration restoration.

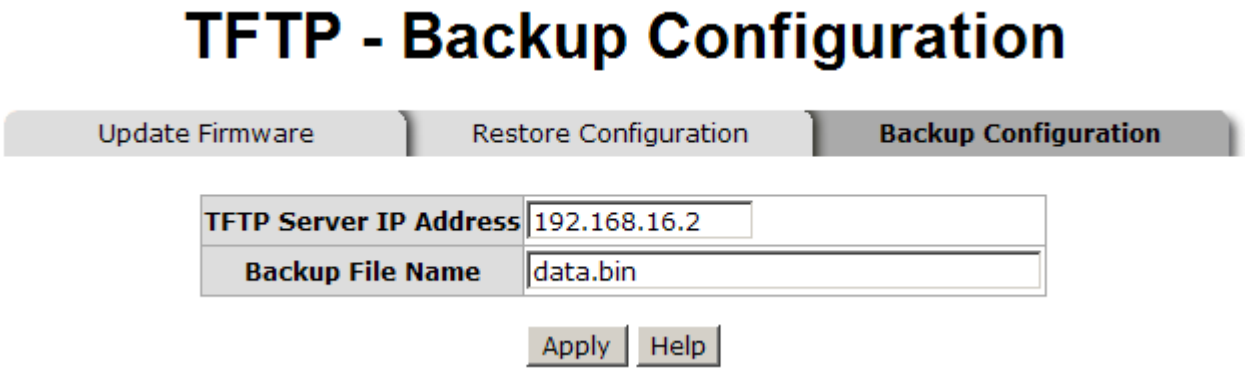


Restore Configuration interface

Backup Configuration

You can back up the current configuration from flash ROM to the TFTP server for the purpose of recovering the configuration later. It helps you avoid wasting time on configuring the settings by backing up the entire configuration.

- **TFTP Server IP Address:** Type in the IP address of the TFTP server.
- **Backup File Name:** Type in the file name.
- When finished, click Apply to start backing up.



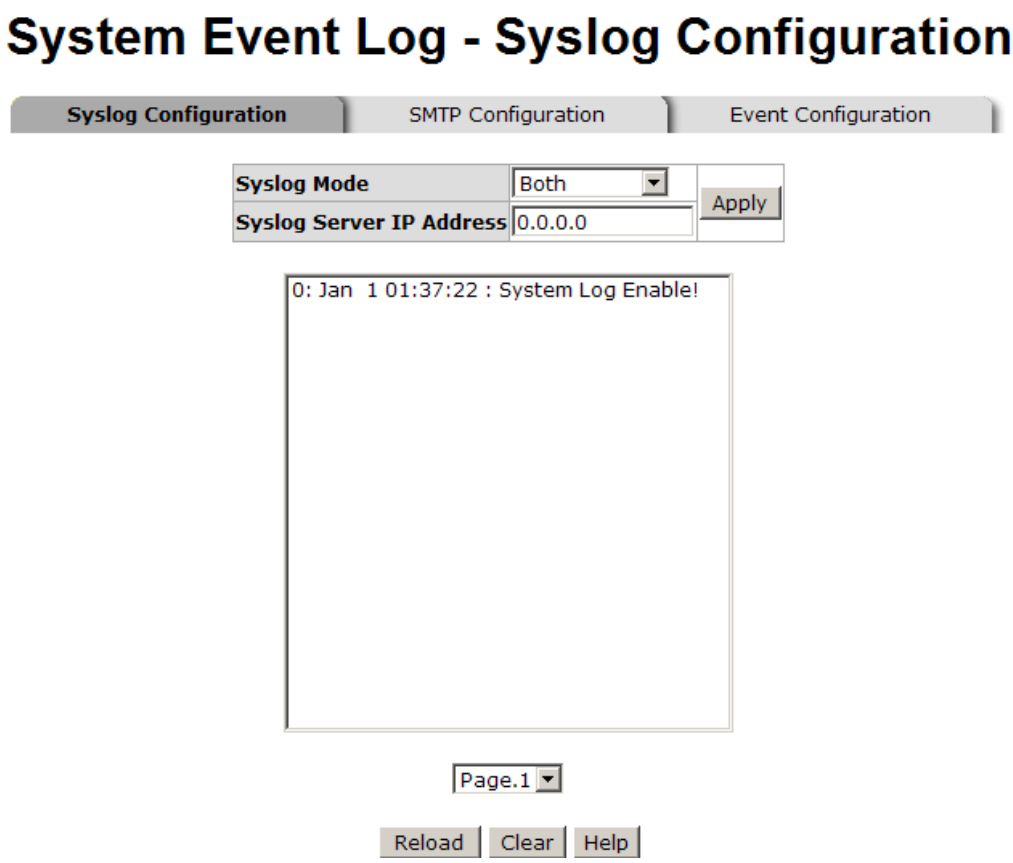
Backup Configuration interface

System Event Log

This page allows the user to decide whether to send the system event log, and select the mode which the system event log will be sent to client only, server only, or both client and server. What kind of event log will be issued to the client/server depends on the selection on the **Event Configuration** tab.

System Event Log—Syslog Configuration

- **Syslog Client Mode:** Select the system log mode—**Client Only**, **Server Only**, or **Both**. ‘Client Only’ means the system event log will only be sent to this interface of the switch, but on the other hand ‘Server Only’ means the system log will only be sent to the remote system log server with its IP assigned. If the mode is set in ‘Both’, the system event log will be sent to the remote server and this interface.
- **Syslog Server IP Address:** When the ‘Syslog Mode’ item is set as Server Only/Both, the user is required to assign the system log server IP address to which the log will be sent.
- Click Reload to refresh the event log displaying area.
- Click Clear to clear the displaying area.
- Make sure the selected mode and IP address, if needed, is correct and click Apply to have the setting take effect.

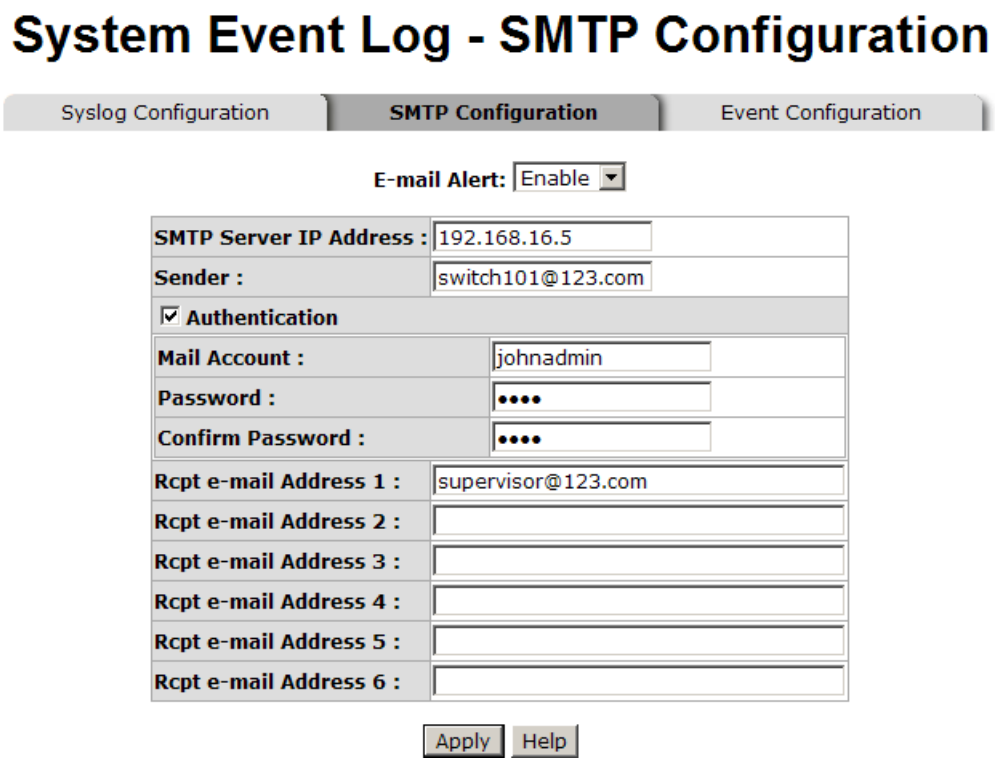


Syslog Configuration interface

System Event Log—SMTP Configuration

Simple Mail Transfer Protocol (SMTP) is the standard for email transmissions across the network. You can configure the SMTP server IP address, sender mail account, password, and the recipient email account to which the e-mail alert will send. Besides, this page provides the authentication mechanism including authentication steps through which the client effectively logs in to the SMTP server during the process of sending e-mail alert.

- **Email Alert:** With this function enabled, the user is allowed to configure the detail settings for sending the e-mail alert to the SMTP server when the events occur.
- **SMTP Server IP Address:** Assign the mail server IP address (when **Email Alert** is enabled, this field will then be available).
- **Sender:** Type in an alias of the switch in complete email address format, e.g. switch101@123.com, to identify where the e-mail alert comes from.
- **Authentication:** Tick the checkbox to have the mail account, password and confirm password fields show up. Configure the email account and password for authentication procedures when this switch logs in to the SMTP server.
- **Mail Account:** Set up the email account, e.g. johnadmin, to receive the email alert. It must be an existing email account on the mail server.
- **Password:** Type in the password to the email account.
- **Confirm Password:** Reconfirm the password.
- **Rcpt e-mail Address 1 ~ 6:** You can also specify up to 6 e-mail accounts to receive the email alert.
- Click Apply to have the configuration take effect.



SMTP Configuration interface

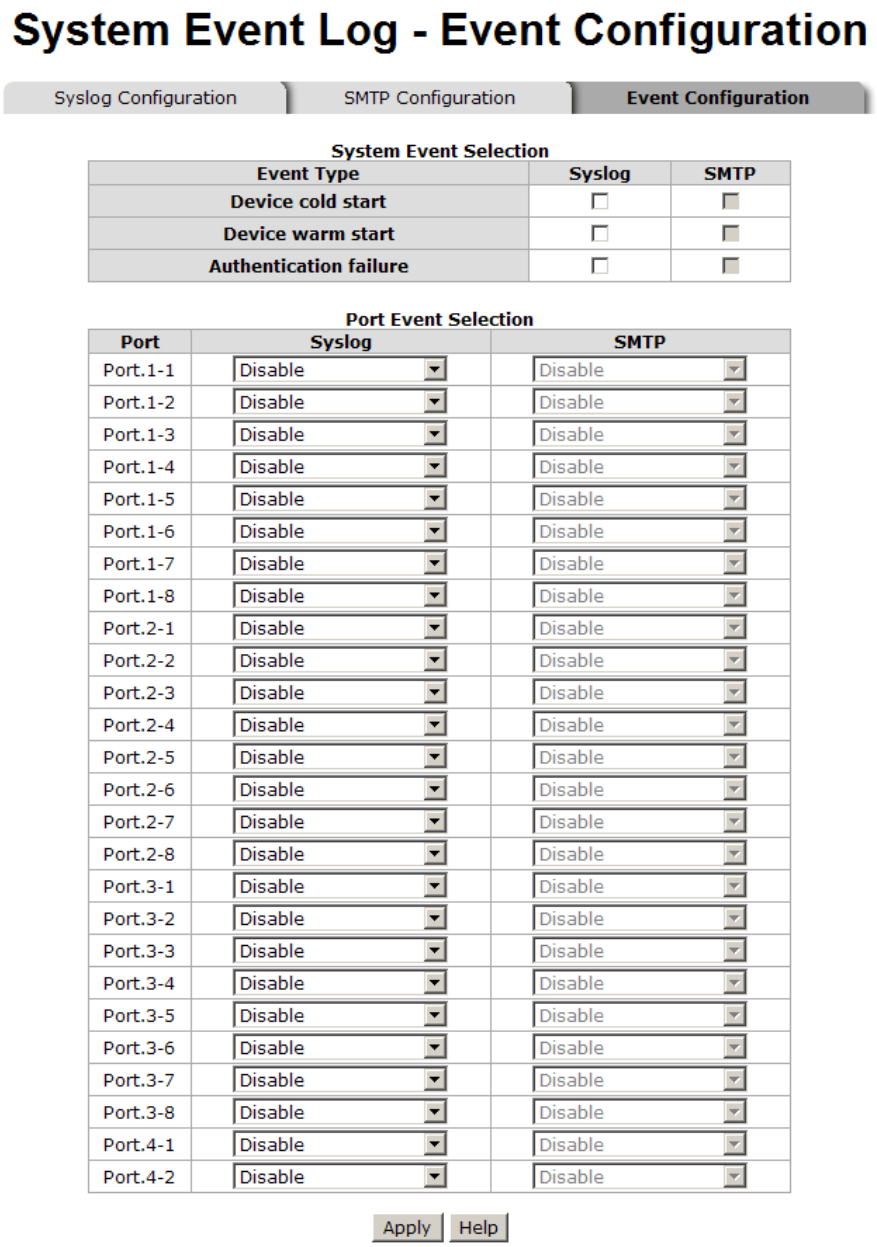
System Event Log—Event Configuration

The checkboxes and pull-down menus are not available unless the **Syslog Client Mode** on the Syslog Configuration tab and the **E-mail Alert** on the SMTP Configuration tab are enabled first.

This tab mainly controls whether an event notification is to be sent to the **Syslog**/**SMTP** server. The part of **System Event Selection** controls the event notification including Device Cold Start, Authentication Failure, and MAC Violation. With the **Syslog**/**SMTP** checkbox ticked, the event log/email alert will be sent to the system log server/SMTP server respectively. As for the part of **Port Event Selection**, port events (link up, link down, and both) can be sent to the system log server/SMTP server by setting the trigger condition for each port respectively.

- **System Event Selection:** There are three event types—*Device Cold Start*, *Device warm start*, and *Authentication Failure*.
  - **Device cold start:** Tick the Syslog/SMTP checkboxes respectively to have the system issue the event log/email alert to the system log/SMTP server when the device executes the cold start action.
  - **Device warm start:** Tick the Syslog/SMTP checkboxes respectively to have the system issue the event log/email alert to the system log/SMTP server when the device executes the warm start action.
  - **Authentication Failure:** When the SNMP authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively.

- **Port event selection:** Each drop-down menu has four options—**Disable**, **Link UP**, **Link Down**, and **Link UP & Link Down**. Disable means no event will be sent to the system log/SMTP server.
  - **Link UP:** The system will issue a log message only when the link-up event of the port occurs.
  - **Link Down:** The system will issue a log message only when the link-down event of port occurs.
  - **Link UP & Link Down:** The system will issue a log message at the time when port connection is link-up and link-down.



Event Configuration interface

SNTP Configuration

SNTP (Simple Network Time Protocol) is a simplified version of NTP which is an Internet protocol used to synchronize the clocks of computers with some time reference. Because time usually just advances, the time on different node stations might be different. With the communicating programs running on those devices, it would cause time to jump forward and back, a non-desirable effect. Therefore, the switch provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet and the local clock in each participating subnet peer.

Daylight Saving Time (DST) is the convention of advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

- **SNTP Client:** Enable/disable the SNTP function to get the time from the SNTP server.
- **Daylight Saving Time:** This function is used to enable/disable *Daylight Saving Period* and *Daylight Saving Offset* fields.
- **UTC Timezone:** Set the location time zone for the switch. The following table lists different location time zones for your reference.

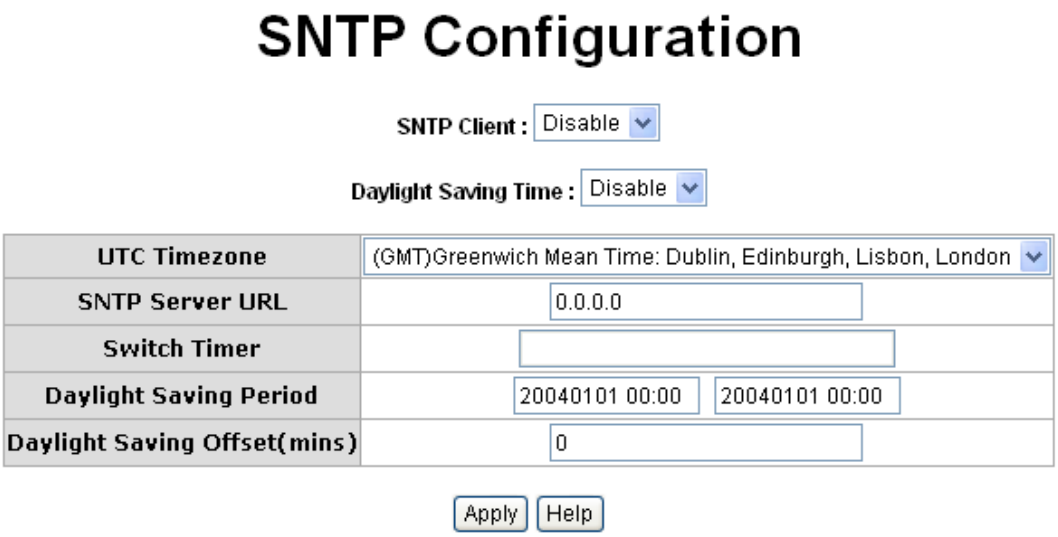
Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am

CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm

JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

- **SNTP Sever URL:** Specify the SNTP server IP address. You can assign a local network time server IP address or an internet time server IP address.
- **Switch Timer:** When the switch has successfully connected to the SNTP server whose IP address was assigned in the field of **SNTP Server URL**, the current coordinated time is displayed here.
- **Daylight Saving Period:** Set up the start and end date/time of the daylight saving period. Please key in the value in the format of 'YYYYMMDD' and 'HH:MM' (leave a space between 'YYYYMMDD' and 'HH:MM').
  - **YYYYMMDD:** an eight-digit year/month/day specification.
  - **HH:MM:** a five-digit (including a colon mark) hour/minute specification.

  For example, key in '20070701 02:00' and '20071104 02:00' in the two fields respectively to represent that DST begins at 2:00 a.m. on March 11, 2007 and ends at 2:00 a.m. on November 4, 2007.
- **Daylight Saving Offset (mins):** For non-US and European countries, specify the amount of time for day light savings. Please key in the valid figure in the range of minute between 0 and 720, which means you can set the offset up to 12 hours.
- Click Apply to have the configuration take effect.



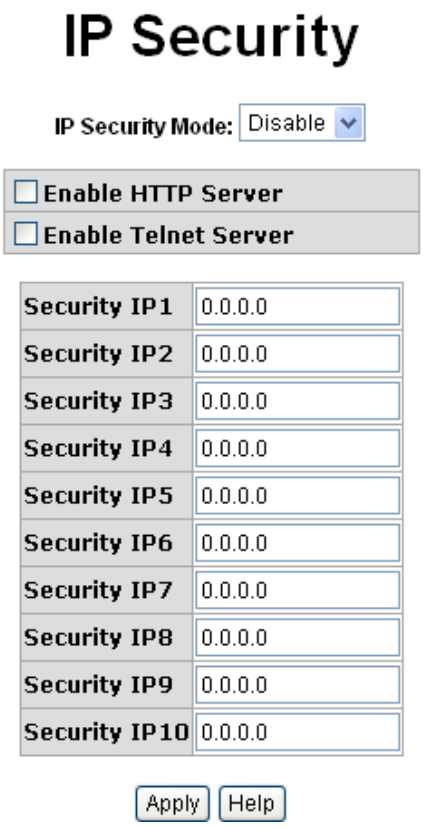
SNTP Configuration interface

IP Security

IP security function allows the user to assign up to 10 specific IP addresses that have permission to manage the switch through the http and telnet services for securing switch management. The purpose of giving permission to limited IP addresses is to allow only the authorized personnel/device to do the management task on the switch.

- **IP Security Mode:** With this selection item set in the **Enable** mode, the **Enable HTTP Server**, **Enable Telnet Server** checkboxes and the ten security IP fields will then be available. If not, those items will appear in grey.
- **Enable HTTP Server:** With this checkbox ticked, Ethernet devices whose IP addresses match any one of the ten IP addresses in the Security IP table will be given permission to access this switch via the HTTP service.
- **Enable Telnet Server:** With this checkbox ticked, Ethernet devices whose IP addresses match any one of the ten IP addresses in the Security IP table will be given permission to access this switch via the telnet service.
- **Security IP 1 ~ 10:** The system allows the user to assign up to 10 specific IP addresses for access security. Only when **IP Security Mode** is enabled can these 10 IP addresses access and manage the switch through the HTTP/Telnet services.
- And then, click Apply to have the configuration take effect.

[NOTE]	Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when the switch powers off.



IP Security interface

User Authentication

The User Authentication interface allows users to configure login user account and password for security reasons.

- **User Name:** The user account is ***root*** by default. Type in the User Name field with a new name as you wish.
- **New Password:** The password to the user account is ***root*** by default. Type in the New Password field with a new password as you wish.
- **Confirm password:** Type in the new password again for confirmation.
- When finished, click Apply to have the configuration take effect.

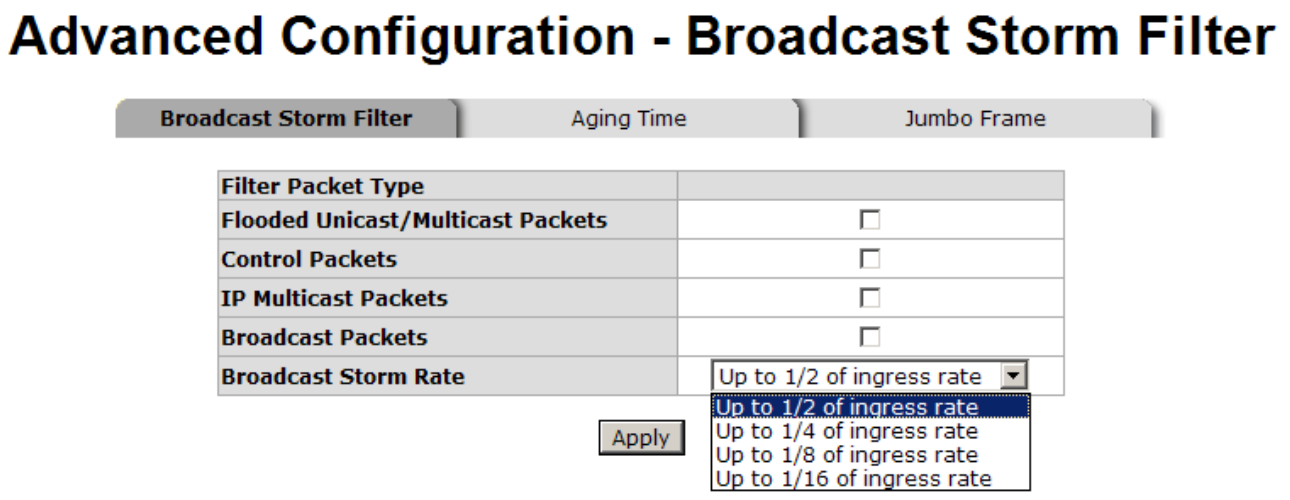
User Authentication interface

Advanced Configuration

Broadcast Storm Filter

This tab allows users to enable the broadcast storm filter for the specific packet type. Tick the checkboxes respectively to enable the filters.

- **Flooded Unicast/Multicast Packets:** When this check box is ticked, the switch will filter the packet type of **Flooded Unicast/Multicast**.
- **Control Packets:** When this checkbox is ticked, the switch will filter the **Control** packet.
- **IP Multicast Packets:** When this checkbox is ticked, the switch will filter the **IP Multicast** packet.
- **Broadcast Packets:** When this checkbox is ticked, the switch will filter the **Flooded Unicast/Multicast** packet.
- **Broadcast Storm Rate:** Users can set theingress filtering rate ranging from 1/2 to 1/16.
- And then, click Apply to have the configuration take effect.

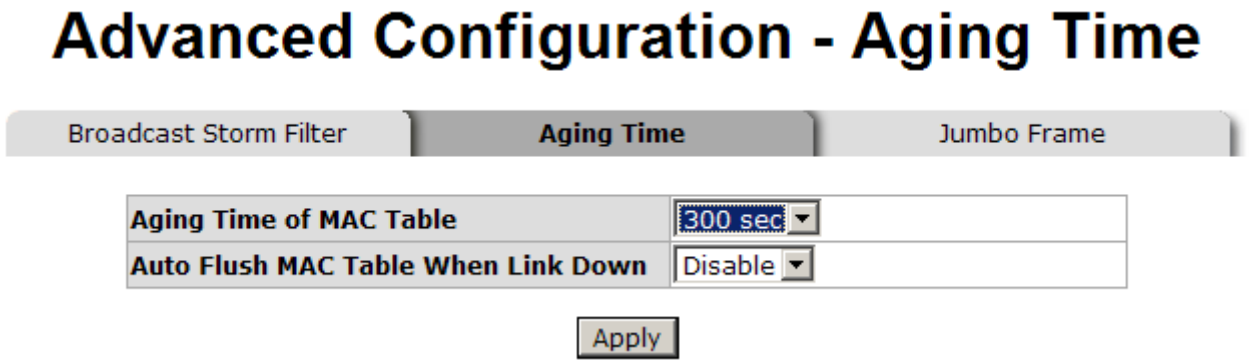


Broadcast Storm Filter

Aging Time

This tab is used to assign the aging time of the MAC table.

- **Aging Time of MAC Table**: Set the aging time on OFF, 150 sec, 300 sec, or 600 sec. When MAC table is not used within the aging time, the MAC address table will then be cleared.
- **Auto Flush MAC Table When Link Down**: When this item is enabled, the switch will flush its MAC address table when connection links down.
- Click Apply to have the configuration take effect.

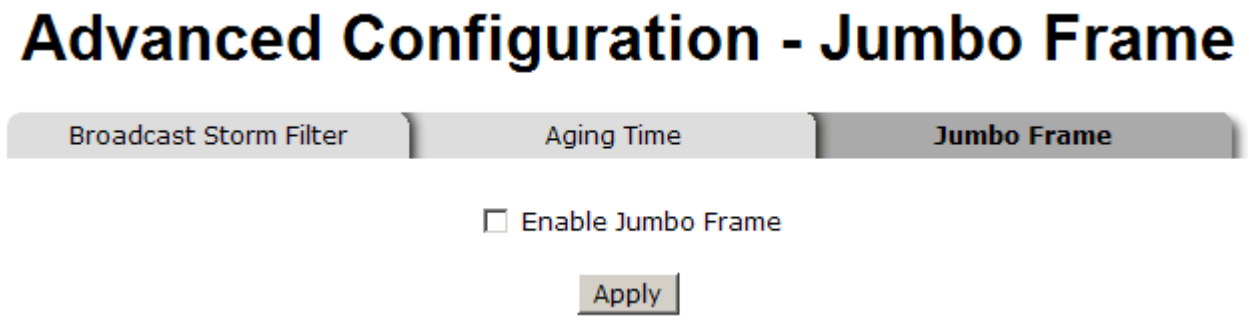


Aging Time Setting

Jumbo Frame

This tab is used to enable the jumbo frame function.

- **Enable Jumbo Frame**: When the checkbox is ticked, the Gigabit port of the switch (on the rear panel) will enlarge the frame size to 9022bytes.
- Click the Apply button to have the configuration effect.



Jumbo Frame Setting

Port Statistics

The following chart provides the current statistics information which displays the real-time packet transfer states for each port. The user might use the information to plan and implement the network, or check and find the problem when the collision or heavy traffic occurs.

- Click the Clear button to clean all counts.

Port Statistics

Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.1-1	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.1-2	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.1-3	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.1-4	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.1-5	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.1-6	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.1-7	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.1-8	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.2-1	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.2-2	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.2-3	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.2-4	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.2-5	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.2-6	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.2-7	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.2-8	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.3-1	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.3-2	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.3-3	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.3-4	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.3-5	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.3-6	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.3-7	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.3-8	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.4-1	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.4-2	1GTX/mGBIC	Up	Enable	10318	0	78727	0	0	0	42516	42795	4254

Clear Help

Port Statistics interface

Port Control

In Port Control you can configure the settings of each port to control the connection parameters.

- **Port:** Scroll up/down the scroll bar and click on the port number to choose a particular port to be configured.
- **State:** Enable/disable the port. If the port state is set on ‘Disable’, the port will not be able to receive or transmit any packet.
- **Negotiation:** Options include Auto and Force. With this parameter set on *Auto*, the speed and duplex fields display in grey, which means the port are negotiated automatically. When you set it on *Force*, you have to set the speed and duplex mode manually by clicking the pull-down menus of the Speed and Duplex fields.
- **Speed:** It is available for selecting when the Negotiation field is set on Force. When the Negotiation field is set on Auto, this field becomes a read-only field displaying in grey.
- **Duplex:** It is available for selecting when the Negotiation field is set on Force. When the Negotiation field is set on Auto, this field becomes a read-only field displaying in grey.
- **Flow Control:** Whether the receiving node sends feedback to the sending node is determined by this item. With this item enabled, if the input data rate of the receiving device exceeds, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. With this item disabled, the receiving device will drop the packets it is unable to process.
- **Security:** When the Security selection is set as ‘**On**’, any access from the device which connects to this port will be blocked unless the MAC address of the device is included in the static MAC address table. Keep in mind that the Security item is set as *On* so that the MAC violation event log/email alert will then be issued. Further information please see the segments of **MAC Address Table—Static MAC Addresses** and **System Event Log—Event Configuration**.
- Click Apply to have the configuration take effect.

Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.1-1 Port.1-2 Port.1-3 Port.1-4	Enable	Auto	100	Full	Enable	Off

Apply Help

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.1-1	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.1-2	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.1-3	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.1-4	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.1-5	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.1-6	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.1-7	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.1-8	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.2-1	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.2-2	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.2-3	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.2-4	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.2-5	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.2-6	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.2-7	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.2-8	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.3-1	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.3-2	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.3-3	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.3-4	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.3-5	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.3-6	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.3-7	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.3-8	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.4-1	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.4-2	N/A	1GTX/mGBIC	Up	Enable	Auto	1G Full	100 Full	Enable	OFF	OFF

Port Control interface

Port Trunk

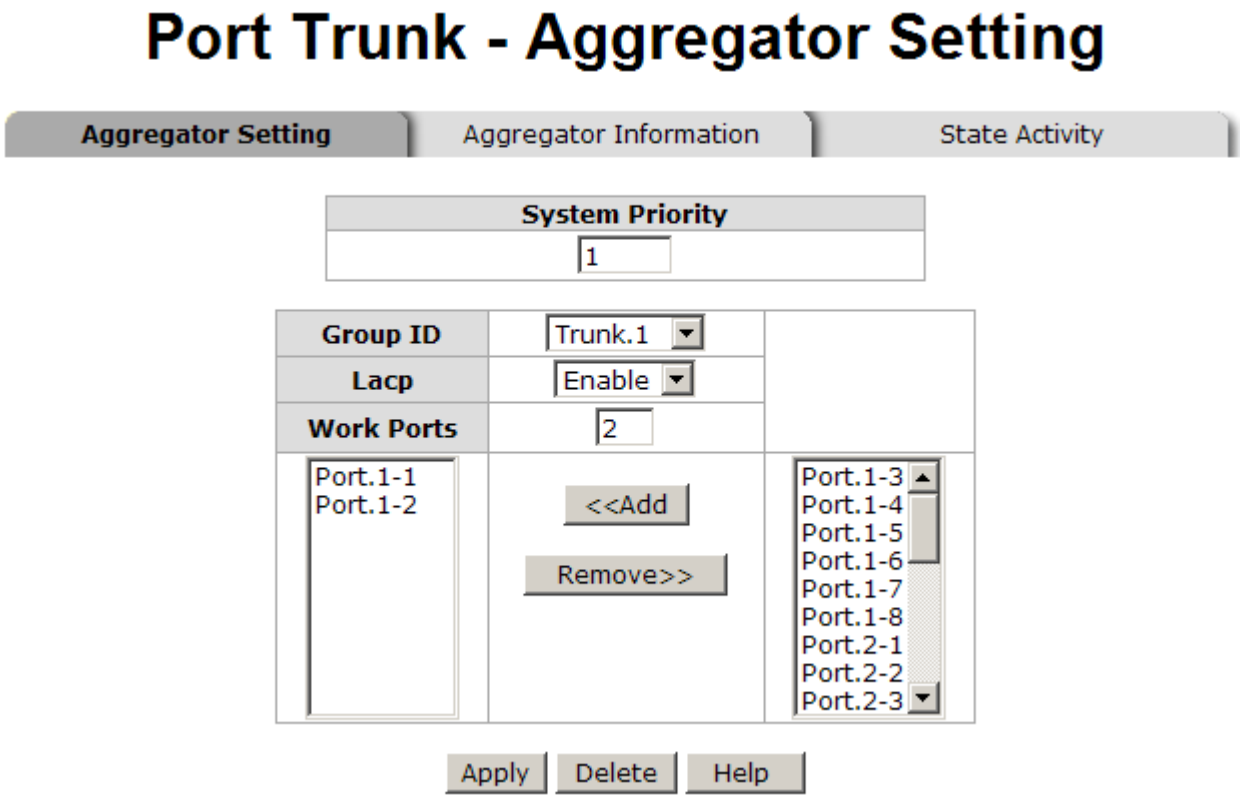
Port trunking is the combination of several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. Link Aggregation Control Protocol (LACP), which is a protocol running on layer 2, provides a standardized means in accordance with IEEE 802.3ad to bundle several physical ports together to form a single logical channel. All the ports within the logical channel or so-called logical aggregator work at the same connection speed and LACP operation requires full-duplex mode.

Aggregator setting

Please read the instrutions below to make an LACP or non-LACP trunk group.

- **System Priority:** A value which is used to identify the controlling switch of an LACP link system. The switch with the lower value has the higher system priority and is selected as the controlling end, which controls port priorities, of the LACP link system.
- **Group ID:** There are four trunk groups to be selected. Assign the group ID to the particular trunk group.
- **LACP:** Click the pull-down menu to enable/disable LACP for the trunk group. With LACP enabled, a port which joins an **LACP trunk group** has to make an agreement with its member ports first. Please notice that a trunk group, including member ports split between two switches, has to enable the LACP function of the two switches. When disabled, the trunk group is a **static trunk group**. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports; but member ports won't know that they should be aggregated together to form a logic trunk group.
- **Work Ports:** This field allows the user to type in the total number of active ports up to four. With a **LACP trunk group** employed, for example you assign four ports to be the members of a trunk group whose *Work Ports* field is set as two the excessive ports will be standby/redundant ports and can be aggregated instead of working ports that fail. As for the **static trunk group** (non-LACP), the number of work ports must equal the total number of the group member ports.

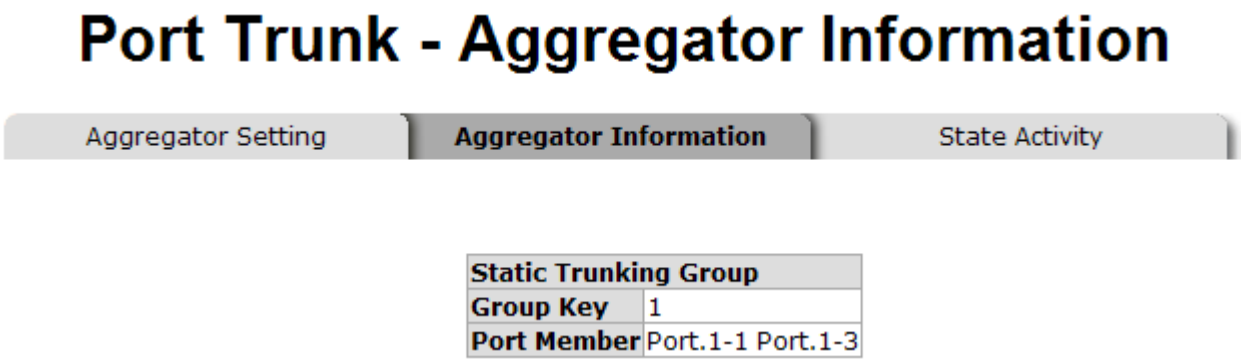
- The system allows a maximum of four ports to be aggregated in a trunk group. Having configured the parameters above, highlight the ports in the right list box to join the trunk group. Click the Add button and the ports highlighted in the right list box will be shifted to the left list box. To remove unwanted ports, select the ports in the left list box and click the Remove button.
- When LACP enabled, you can configure LACP Active/Passive states for each member port on the **State Activity** tab.
- When finished, click Apply to take the configuration take effect.
- To remove a trunk group, select the Group ID by clicking the pull-down menu labeled as 'Group ID' and click then click the Delete button.



Port Trunk—Aggregator Setting interface

Aggregator Information

When you have set the LACP aggregator, you will see the related information here.



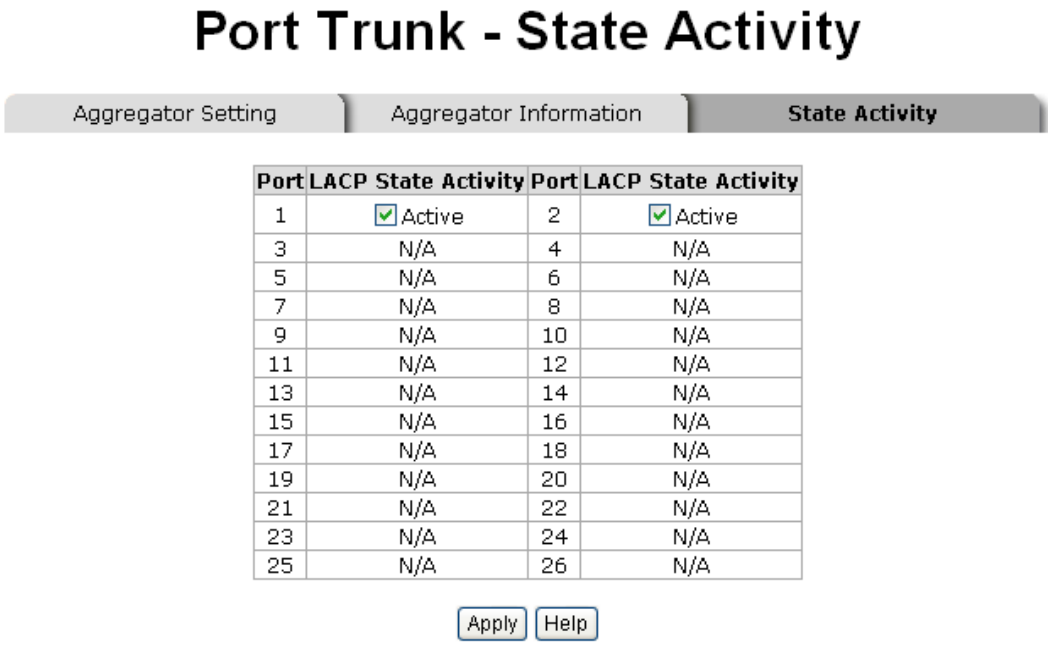
Port Trunk – Aggregator Information interface

State Activity

Having configured the LACP aggregator on the **Aggregator Setting** tab, you may want to change the state activity for the members of the LACP trunk group. You can tick/untick the checkbox beside the state label. If you remove the tick mark of the corresponding port and click the Apply button, the port state activity will change to **Passive**.

- **Active:** The port automatically sends LACP protocol packets.
- **Passive:** The port does not actively send LACP protocol packets. It responds only if it receives LACP protocol packets from the opposite device.

[NOTE]	**A link** having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.

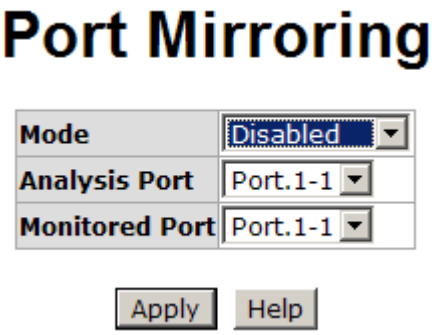


Port Trunk – State Activity interface

Port Mirroring

Port Mirroring is a method for monitoring of network traffic on switched networks. Traffic through ports can be monitored by one specific port, which means traffic going in or out the monitored (source) ports will be duplicated into the analysis (mirroring) port.

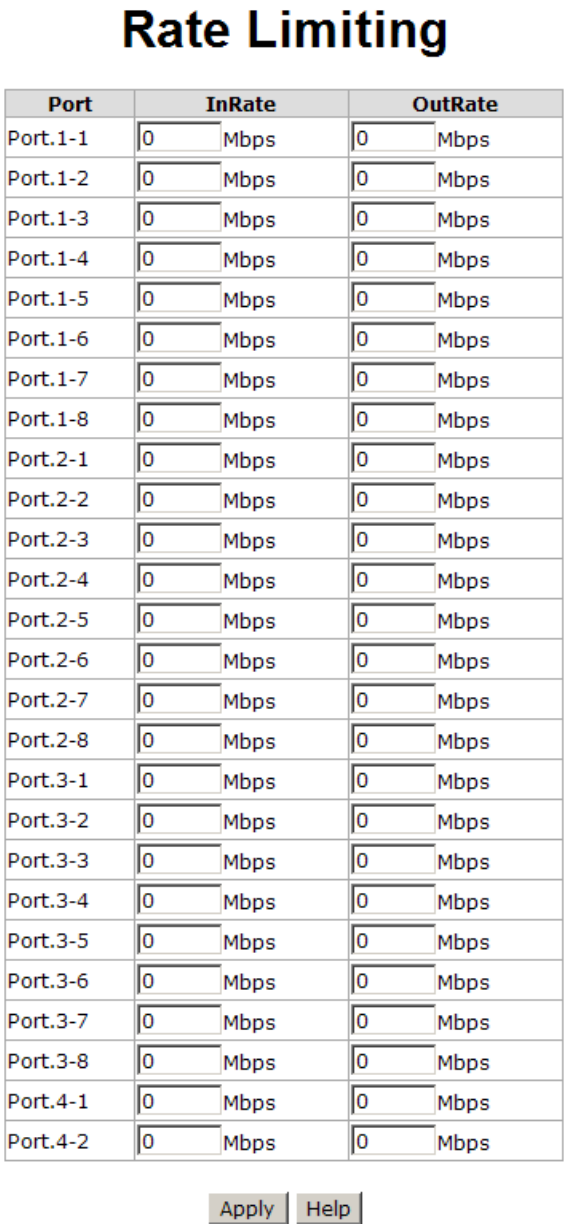
- **Mode:** Select the mirroring mode by clicking the pull-down menu: **RX**, **TX or Both RX/TX.**
- **Analysis Port:** Select one port to be the analysis (mirroring) port for monitoring RX only, TX only or both RX and TX traffic which come from source port. Users can forward the traffic captured by the analysis port to the packet analyzer like Netxray for further analyses.
- **Monitored Port:** Select the port that you want to monitor. All monitored port traffic will be copied to analysis (mirroring) port. Users can select one monitored port by clicking the pull-down menu.
- When finished, click the Apply button.



Port Trunk – Port Mirroring interface

Rate Limiting

You can respectively configure the ingress/egress rate for each port.


Rate Limiting
Port
InRate
OutRate
Port.1-1 0 Mbps 0 Mbps
Port.1-2 0 Mbps 0 Mbps
Port.1-3 0 Mbps 0 Mbps
Port.1-4 0 Mbps 0 Mbps
Port.1-5 0 Mbps 0 Mbps
Port.1-6 0 Mbps 0 Mbps
Port.1-7 0 Mbps 0 Mbps
Port.1-8 0 Mbps 0 Mbps
Port.2-1 0 Mbps 0 Mbps
Port.2-2 0 Mbps 0 Mbps
Port.2-3 0 Mbps 0 Mbps
Port.2-4 0 Mbps 0 Mbps
Port.2-5 0 Mbps 0 Mbps
Port.2-6 0 Mbps 0 Mbps
Port.2-7 0 Mbps 0 Mbps
Port.2-8 0 Mbps 0 Mbps
Port.3-1 0 Mbps 0 Mbps
Port.3-2 0 Mbps 0 Mbps
Port.3-3 0 Mbps 0 Mbps
Port.3-4 0 Mbps 0 Mbps
Port.3-5 0 Mbps 0 Mbps
Port.3-6 0 Mbps 0 Mbps
Port.3-7 0 Mbps 0 Mbps
Port.3-8 0 Mbps 0 Mbps
Port.4-1 0 Mbps 0 Mbps
Port.4-2 0 Mbps 0 Mbps
Apply
Help

Rate Limiting interface

- All the ports support packet ingress and egress rate control.
  - **InRate:** Enter the port effective ingress rate (The default value is “0”).
  - **OutRate:** Enter the port effective egress rate (The default value is “0”).
- When finished, click Apply to have the configuration take effect.

VLAN Configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which allows you to isolate network traffic. Therefore only the members of the same VLAN will receive traffic from the ones among the same VLAN. Basically, creating a VLAN on a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch; however, all the network devices are still plugged into the same switch physically.

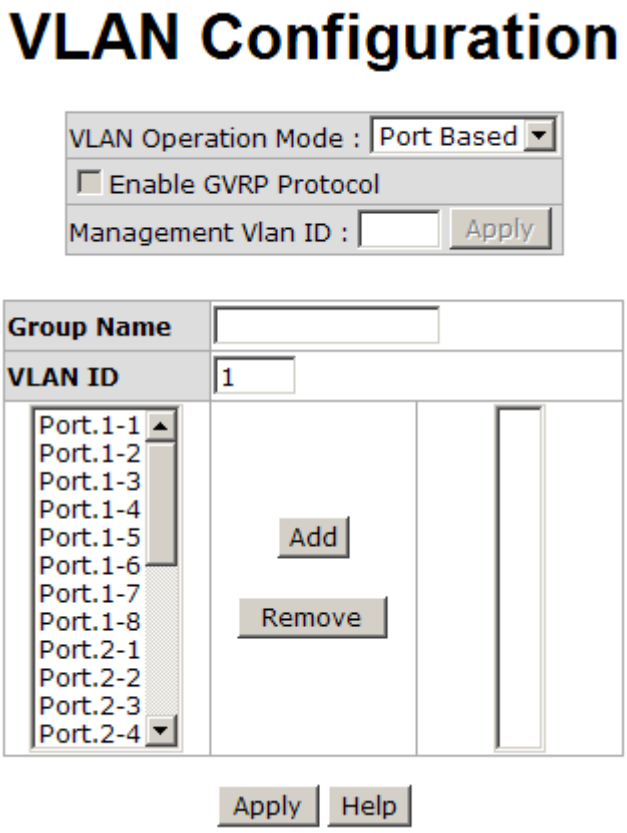
This switch supports **Port-based** and **802.1Q** (tagged-based) VLAN. Please read the following instructions to configure the appropriate type of VLAN for your need.

Port-based VLAN

A port-based VLAN normally consists of its members—ports, which means the VLAN is created by grouping the selected ports. This method provides the convenience for users to configure a simple VLAN easily without complicated steps. Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN that is, technically, a single broadcast domain. If the port-based VLAN is enabled, the VLAN-tagging will be ignored. Port-based VLAN allows the user to create separate VLANs to limit the unnecessary packet flooding; however, for the purpose of sharing resource, a single port called a common port can belongs to different VLANs, which all the member devices (ports) in different VLANs have the permission to access the common port while they still cannot communicate with each other in different VLANs.

VLAN – Port Based interface

- Click Add to create a new VLAN group (The VLAN groups can be up to 64).



VLAN—Port Based Add interface

- Enter the group name and VLAN ID. Select the port number available in the left list

box, and click the Add button to move the highlighted ports to the right list box. Or you can select any of the ports listed in the right field and click Remove to remove port(s) from the VLAN.

- When finished, click Apply to have the VLAN configuration take effect.
- And then you will see the VLAN list shows up.
- With the VLAN list box showing up, select VLAN(s) and click the Delete button to get rid of the VLAN(s).
- Highlight a VLAN and click the Edit button to change group name, VLAN ID, or to add/remove the members of the existing VLAN group.

[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will lose when the switch powers off.

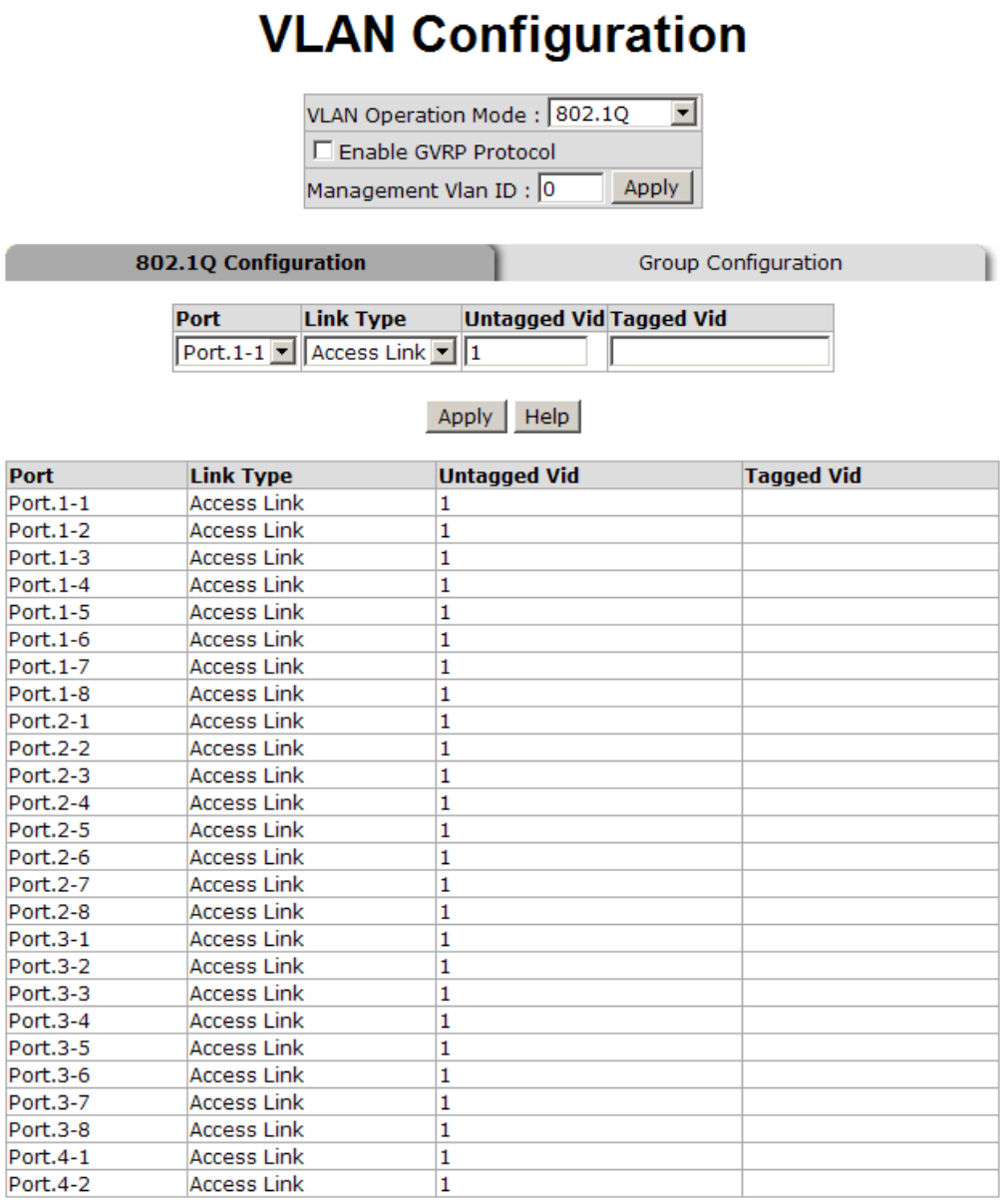
802.1Q VLAN

When the VLAN operation mode is set on 802.1Q, all ports on the switch belong to the default VLAN of VID 1, which means they logically are regarded as members of the same broadcast domain. The valid VLAN ID is in the range of number between 1 and 4094. The amount of VLAN groups is up to 256 including the default VLAN that cannot be deleted.
GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of VLANs within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices. For example, with GVRP enabled, the switches are able to automatically exchange the information of their VLAN database. Therefore, the user needn't manually configure the link type. The packets belonging to the same VLAN can communicate across switches.
Each member port of 802.1Q is on either an Access Link (VLAN-tagged) or a Trunk Link (no VLAN-tagged). All frames on an Access Link carry no VLAN identification. Conversely, all frames on a Trunk Link are VLAN-tagged. Besides, there is the third mode—Hybrid. A Hybrid Link can carry both VLAN-tagged frames and untagged frames. A single port is supposed to belong to a particular VLAN group, except it is on a Trunk/Hybrid Link.
The technique of 802.1Q tagging inserts a 4-byte tag, including VLAN ID of the destination port—PVID, in the frame. With the combination of Access/Trunk/Hybrid Links, the communication across switches also can make the packet sent through tagged and untagged ports.

Please follow the instructions below to configure the 802.1Q VLAN.

- Click the pull-down menu to select **802.1Q** and click Apply to configure the VLAN Operation Mode on **802.1Q**.
- **Enable GVRP Protocol:** Tick this checkbox to enable GVRP protocol. This checkbox is available while the VLAN Operation Mode is set on **802.1Q**.
- **Management VLAN ID:** Only the VLAN members, whose Untagged VID (PVID) equals to the value specified in this field, have permission to access the switch. The default value is '0' that means this limit is not enabled (all members in different VLANs can access this switch).

- After you have configured the three parameters, click the Apply button right beneath this area to finish creating an 802.1Q VLAN.



Port	Link Type	Untagged Vid	Tagged Vid
Port.1-1	Access Link	1	
Port.1-2	Access Link	1	
Port.1-3	Access Link	1	
Port.1-4	Access Link	1	
Port.1-5	Access Link	1	
Port.1-6	Access Link	1	
Port.1-7	Access Link	1	
Port.1-8	Access Link	1	
Port.2-1	Access Link	1	
Port.2-2	Access Link	1	
Port.2-3	Access Link	1	
Port.2-4	Access Link	1	
Port.2-5	Access Link	1	
Port.2-6	Access Link	1	
Port.2-7	Access Link	1	
Port.2-8	Access Link	1	
Port.3-1	Access Link	1	
Port.3-2	Access Link	1	
Port.3-3	Access Link	1	
Port.3-4	Access Link	1	
Port.3-5	Access Link	1	
Port.3-6	Access Link	1	
Port.3-7	Access Link	1	
Port.3-8	Access Link	1	
Port.4-1	Access Link	1	
Port.4-2	Access Link	1	

802.1q VLAN interface

- On the 802.1Q Configuration tab, click the *Port* pull-down menu to select a port you want to configure within the VLAN.
- **Link Type**: Three options are available. Click the pull-down menu to select the link type.
  - **Access Link:** A segment which provides the link path for one or more stations to the VLAN-aware device like switches. An Access Port (untagged port) connecting to the access link has an untagged VID (also called PVID). After an

untagged frame gets into the access port, the switch inserts a four-byte tag in the frame. The contents of the last 12-bit of the tag is the untagged VID. When this frame is sent out through any of the access ports of the same PVID, the switch will remove the tag from the frame to recover it to what it was. Those ports of the same untagged VID are regarded as the same VLAN group members.

[NOTE] *Because the access port doesn't have an understanding of tagged frame, the field of Tagged VID is not available.*

- **Trunk Link:** A segment which provides the link path for one or more VLAN-aware devices. A Trunk Port connecting to the trunk link has an understanding of tagged frame, which is used for communications across VLANs. Which frames of the specified VIDs will be forwarded depends on the values filled in the Tagged VID field. Please insert a comma between two VIDs.

[NOTE]

1. *A trunk port doesn't insert tags into an untagged frame, and therefore the untagged VID field is not available.*
2. *It's not necessary to type '1' in the tagged VID field. The trunk port will forward the frames of VLAN 1.*
3. *The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.*

- **Hybrid Link:** A segment which consists of Access and Trunk links. The hybrid port has both the features of the access and trunk ports. A hybrid port has a PVID belonging to a particular VLAN, and also forwards the specified tagged-frames for the purpose of VLAN communications between switches.

[NOTE]

1. *It's not necessary to type '1' in the tagged VID field. The hybrid port will forward the frames of VLAN 1.*
2. *The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.*

- **Untagged Vid:** This field is available when the *Link Type* pull-down menu is set on

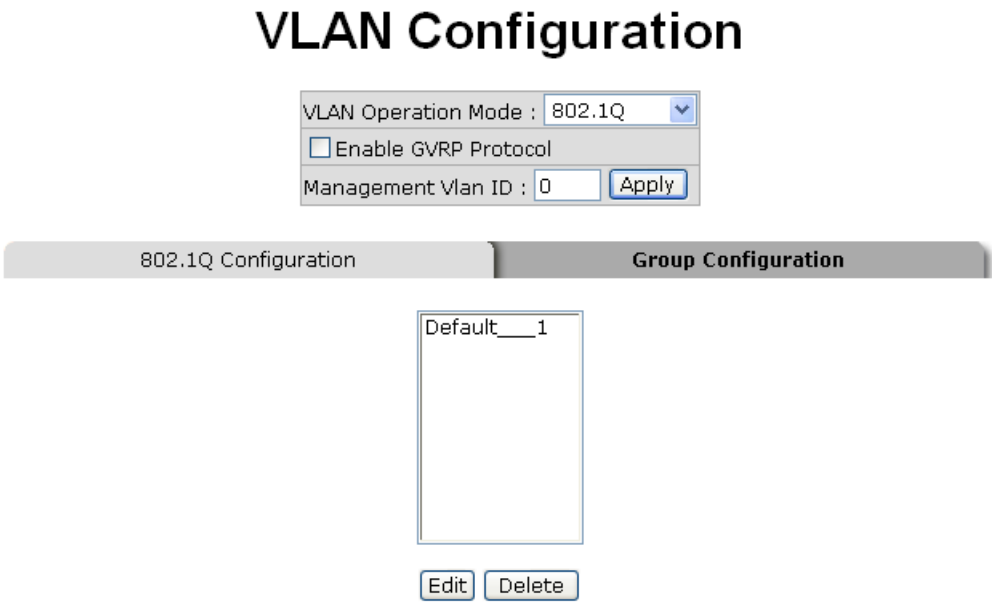
Access Link and *Hybrid Link*. Assign a number in the range between 1 and 4094.

- **Tagged Vid:** This field is available when the *Link Type* pull-down menu is set on *Trunk Link* and *Hybrid Link*. Assign a number in the range between 1 and 4094.
- Click the Apply button on the tab to have the port configuration take effect.
- And then you can see the link type, untagged VID, and tagged VID information of each port shown in the table on the screen.

Group Configuration

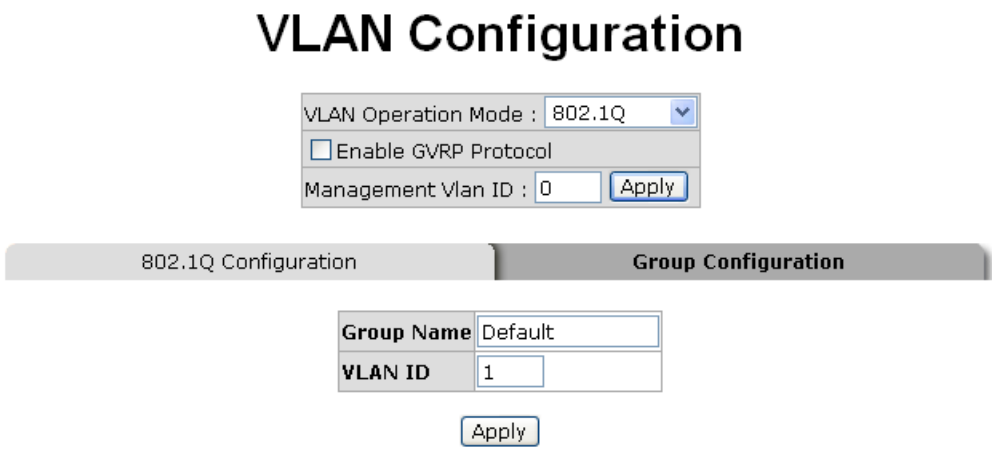
Edit the existing VLAN Groups.

- Click the Group Configuration tab.
- Select a VLAN group in the list box and click the Edit button.



Group Configuration interface

- After clicking the Edit button, you can change group name and VLAN ID of the selected VLAN group.



Group Configuration interface

- When finished, click Apply to have the modification take effect.

Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol providing for faster spanning tree convergence after a topology change. The system also supports STP and will auto-detect the connected device running STP or RSTP.

RSTP System Configuration

This tab allows users to configure parameters for RSTP and displays the spanning tree information of the root bridge.

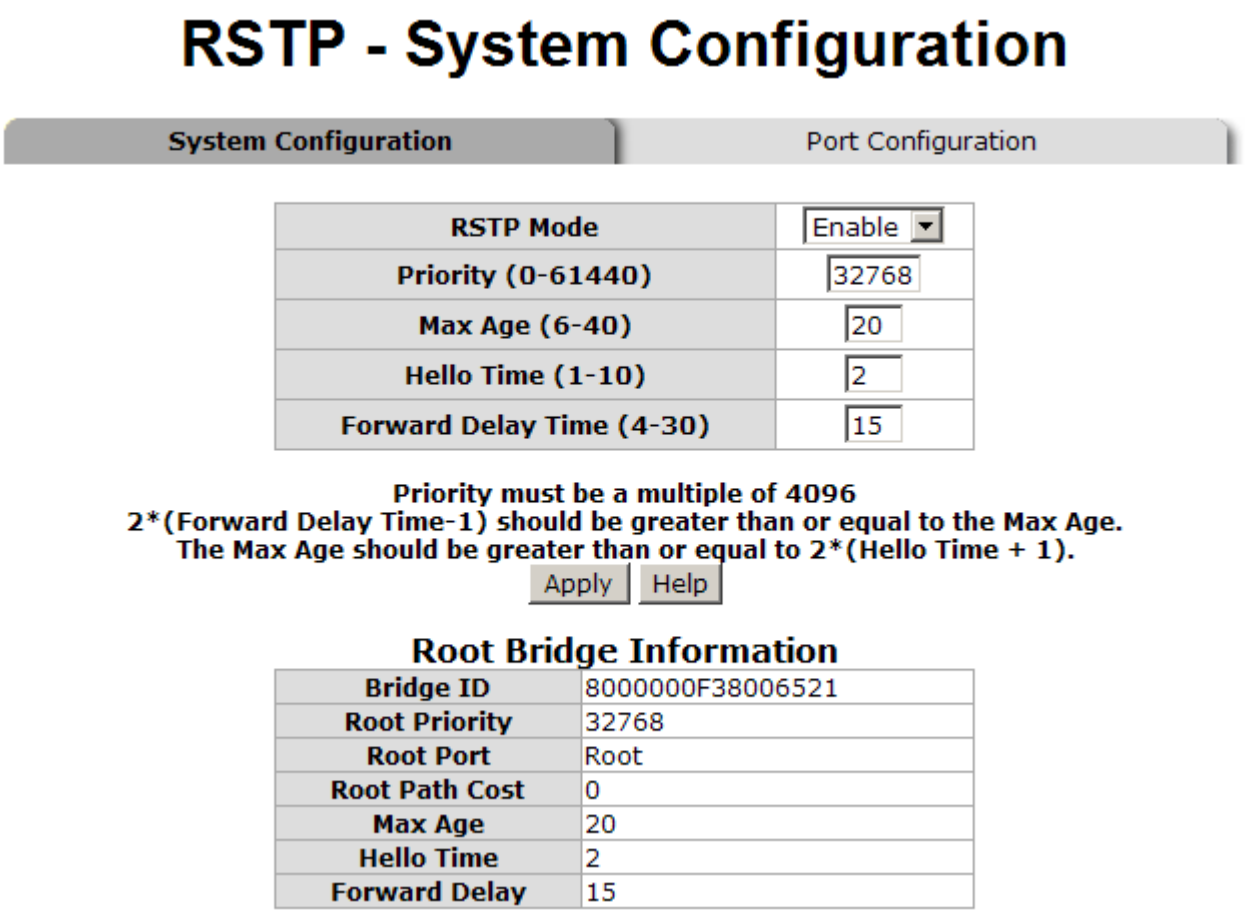
- **RSTP mode:** Click the pull-down menu to enable the RSTP function.
- **Priority (0-61440):** The switch with the lowest numerical value has the highest priority and will be selected as the root device. If the value is changed, users must reboot the switch. Note the value specified in this field must be a multiple of 4096 according to the protocol rule.
- **Max Age (6-40):** Enter the time in seconds between 6 and 40 for which the switch waits to attempt to save its configuration.
- **Hello Time (1-10):** Enter the time in seconds between 1 and 10 that controls the switch to send out the BPDU packet to check current states of RSTP.
- **Forward Delay Time (4-30):** Enter the time in seconds between 4 and 30 that a port spends changing from its learning and listening state to the forwarding state.
- When finished, click the Apply button to have the configuration take effect.

[NOTE]	Follow the rule below to configure *Max Age*, *Hello Time*, and *Forward Delay Time* parameters. **2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)**

Root Bridge Information

The column fields give the current bridge information for the switch.

- **Bridge ID:** This field displays the bridge ID by showing the MAC address of this switch.
- **Root Priority:** This field displays the numerical value indicating bridge priority of the switch. Generally, the switch with the lowest numerical value in the network is set as the root bridge.
- **Root Port:** This field indicates which port is connecting to the root bridge. When the switch is set as the root bridge, the word 'Root' shows here.
- **Root Path Cost:** This field displays the path cost between the switch's root port and the designated port of the root bridge. Path cost is a value to each port typically based on rules described as part of 802.1d. For the root bridge this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.
- **Max Age:** Displays the configured aging time of the switch.
- **Hellow Time:** Displays the configured Hellow Time.
- **Forward Delay:** Displays the configured forward delay time.



RSTP System Configuration interface

Port Configuration

This tab offers the interface for RSTP port configuration where you can assign parameters to each port. The rapid spanning tree protocol will have the port with the higher priority in forwarding state and block other ports to make certain that there is no loop in the LAN.

- Scroll the list box to select a port for configuration.
- **Path Cost:** The path cost can be managed. Enter a number in the range of 1 to 200,000,000.
- **Priority:** Port Poriority. Give the value to decide which port should be blocked by setting its priority. Enter a number between 0 and 240. The entered value must be a multiple of 16.
- **Admin P2P:** The rapid state transitions possible within RSTP are dependent upon whether the port concerned can only be connected to exactly another bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P states of the link to be manipulated administratively. True means the port is regarded as a point-to-point link. False means the port is regarded as a shared link. Auto means the link type is determined by the auto-negotiation between the two peers.
- **Admin Edge:** The port directly connected to an end station is known as an edge port that won't create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" state.
- **Admin Non Stp:** Configure whether the port includes the STP mathematic calculation. **True** means not to include the STP mathematic calculation. **False** means the STP mathematic calculation is included.
- When finished, click Apply to have the configure take effect.

RSTP - Port Configuration

System Configuration | Port Configuration

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
Port.1-1 Port.1-2 Port.1-3 Port.1-4 Port.1-5	20000(	128	Auto	true	false

priority must be a multiple of 16

Apply Help

RSTP Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.1-1	200000	128	True	True	False	Disabled	Disabled
Port.1-2	200000	128	True	True	False	Disabled	Disabled
Port.1-3	200000	128	True	True	False	Disabled	Disabled
Port.1-4	200000	128	True	True	False	Disabled	Disabled
Port.1-5	200000	128	True	True	False	Disabled	Disabled
Port.1-6	200000	128	True	True	False	Disabled	Disabled
Port.1-7	200000	128	True	True	False	Disabled	Disabled
Port.1-8	200000	128	True	True	False	Disabled	Disabled
Port.2-1	200000	128	True	True	False	Disabled	Disabled
Port.2-2	200000	128	True	True	False	Disabled	Disabled
Port.2-3	200000	128	True	True	False	Disabled	Disabled
Port.2-4	200000	128	True	True	False	Disabled	Disabled
Port.2-5	200000	128	True	True	False	Disabled	Disabled
Port.2-6	200000	128	True	True	False	Disabled	Disabled
Port.2-7	200000	128	True	True	False	Disabled	Disabled
Port.2-8	200000	128	True	True	False	Disabled	Disabled
Port.3-1	200000	128	True	True	False	Disabled	Disabled
Port.3-2	200000	128	True	True	False	Disabled	Disabled
Port.3-3	200000	128	True	True	False	Disabled	Disabled
Port.3-4	200000	128	True	True	False	Disabled	Disabled
Port.3-5	200000	128	True	True	False	Disabled	Disabled
Port.3-6	200000	128	True	True	False	Disabled	Disabled
Port.3-7	200000	128	True	True	False	Disabled	Disabled
Port.3-8	200000	128	True	True	False	Disabled	Disabled
Port.4-1	20000	128	True	True	False	Disabled	Disabled
Port.4-2	20000	128	True	True	False	Forwarding	Designated

RSTP Port Configuration interface

Pro-Ring System

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms not the same.

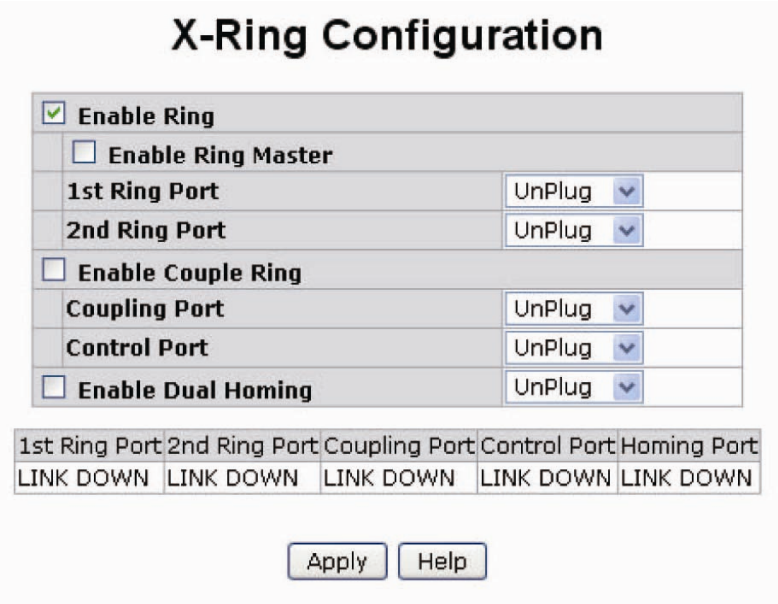
In the X-Ring topology, every switch should enable X-Ring function and assign two member ports in the ring. Only one switch in the X-Ring group would be set as a master switch that would be blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of network connection occurs, the backup port will automatically become a working port to recovery the failure.

The switch supports the function and interface for setting the switch as the ring master or slave mode. The ring master can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, then software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode will be enabled by the X-Ring configuration interface. Also, user can identify the switch as the ring master from the R.M. LED panel of the LED panel on the switch.

The system also supports the coupling ring that can connect 2 or more X-Ring group for the redundant backup function and dual homing function that prevent connection lose between X-Ring group and upper level/core switch.

- **Enable X-Ring:** To enable the X-Ring function. Marking the check box to enable the X-Ring function.
- **Enable Ring Master:** Mark the check box for enabling this machine to be a ring master.
- **1st & 2nd Ring Ports:** Pull down the selection menu to assign two ports as the member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the backup port. When **1st Ring Port** fails, the system will automatically upgrade the **2nd Ring Port** to be the working port.

- **Enable Coupling Ring:** To enable the coupling ring function. Marking the check box to enable the coupling ring function.
- **Coupling port:** Assign the member port.
- **Control port:** Set the switch as the master switch in the coupling ring.
- **Enable Dual Homing:** Set up one of port on the switch to be the Dual Homing port. In an X-Ring group, maximum Dual Homing port is one. Dual Homing only work when the X-Ring function enable.
- And then, click Apply to apply the configuration.



X-ring Interface

[NOTE]

1. When the X-Ring function enable, user must disable the RSTP. The X-Ring function and RSTP function cannot exist at the same time.
2. Remember to execute the 'Save Configuration' action, otherwise the new configuration will lose when switch power off.

X-Ring I Recovery time table	X- Ring	Couple Ring	Dual Homing	Dual Ring	Central Ring
Recovery Time(ms) (Using 1G Fiber Cable or 100Mb Copper Cable)	10	150	150~6000	10	10
Recovery Time(ms) (Using 1G Coppor Cable)	150	150	150~6000	150	150

SNMP Configuration

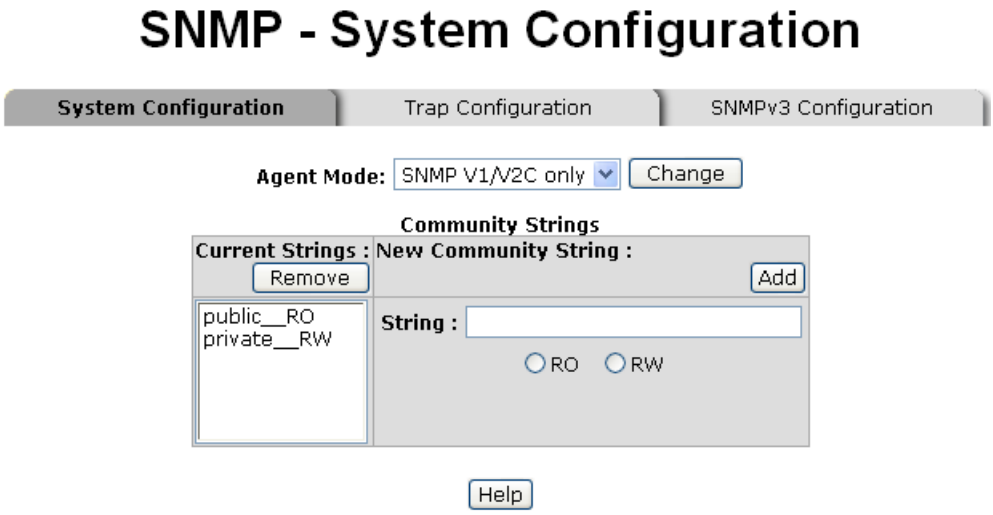
Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems (NMS) learn of problems by receiving traps or change notices from network devices implementing SNMP.

System Configuration

This tab allows users to define new community strings and remove the unwanted community strings for authentication purposes. With adding a new community string, you should also specify the type of access permission and the agent mode.

- **Agent Mode:** Click the pull-down menu to select the SNMP version that the community string will use. And then click the Change button to ensure the selected SNMP version mode is changed.

- **Community Strings:**
  - **String:** Enter the community string in the field as a password for authentication.
  - **RO:** Read only. With this radio button selected, the community string is given the read-only permission for the MIB objects.
  - **RW:** Read/write. With this radio button selected, the community string is given the read/write permission for the MIB objects.
  - Click Add to finish adding a new community string.
  - To remove a specific community string, select the community string shows in the list box and click Remove. The strings of Public_RO and Private_RW are default strings. You can remove them but after resetting the switch to default, the two strings show up again.

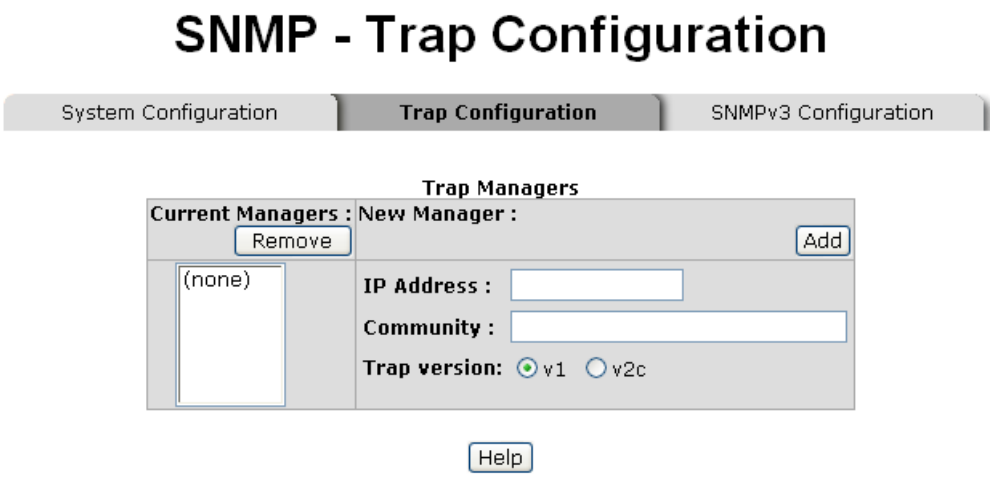


SNMP System Configuration interface

Trap Configuration

A trap manager is a management station that receives trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

- **IP Address:** Enter the IP address of the trap manager.
- **Community:** Enter the community string for the trap station.
- **Trap Version:** Select the SNMP trap version—v1 or v2c.
- When finished, click Add.
- To remove a specific manager station, select the entries listed in the Current Managers field and click Remove.



Trap Managers interface

SNMPV3 Configuration

This tab allows users to configure the SNMPv3 settings for communications via SNMPv3.

Context Table

Configure the SNMPv3 context table. Assign the context name in the field. Click Apply to add the context name added or changed.

User Table

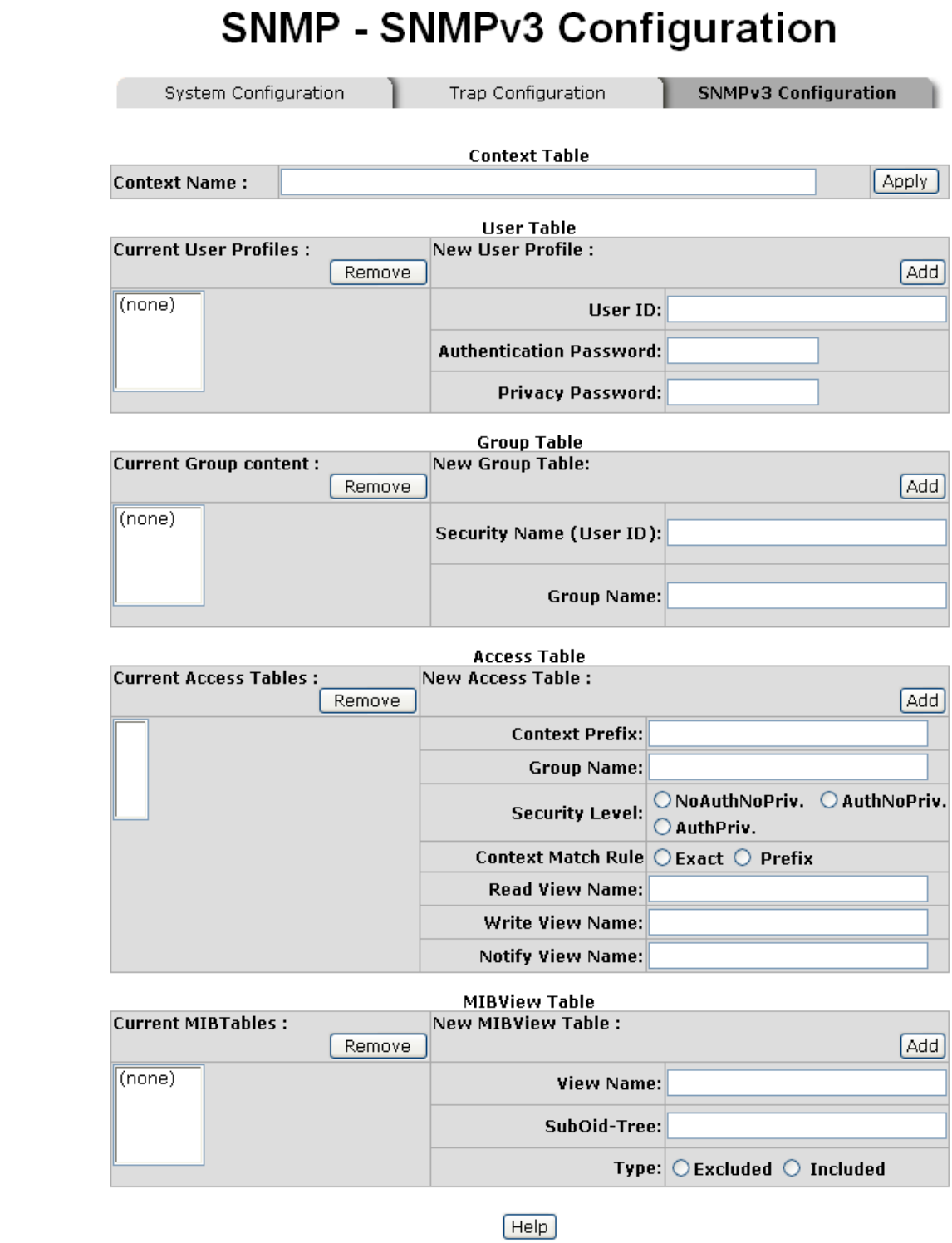
Configure the SNMPv3 user table.

- **User ID:** Type the user name in the field.
- **Authentication Password:** Assign the authentication password to the user ID.
- **Privacy Password:** Assign the private password to the user ID.
- Click the Add button to create a new user profile.
- To remove a user profile, select an entry in the Current User Profiles listbox and click the Remove button to remove the unwanted user profile.

Group Table

Configure the SNMPv3 group table.

- **Security Name (User ID):** Specify the user name that you have set up in the user table.
- **Group Name:** Type the group name in the field.
- Click the Add button to create a new group name
- To remove a group name, select an entry in the Current Group Content listbox and click the Remove button to remove the unwanted group.



SNMP V3 configuration interface

Access Table

Configure the SNMPv3 access table.

- **Context Prefix:** In this filed type in the prefix letters of the context name that is assigned in the context table.
- **Group Name:** Type in the group name that is assigned in the group table.
- **Security Level:** Select a radio button to determine which security level is assigned to the group. The options include:
  NoAuthNoPriv: Communications are made without authentication or encryption.
  AuthNoPriv: Communications are made with authentication but without encryption.
  AuthPriv: Communications are made with authentication and encryption.
- **Context Match Rule:** Select the radio button to determine the context matching rule. You can configure it as a complete matching or prefix matching condition.
- **Read View Name:** Assign permission of reading to a user ID typed that exists in the User Table.
- **Write View Name:** Assign permission of writing to a user ID typed that exists in the User Table.
- **Notify View Name:** Assign permission of notifying to a user ID typed that exists in the User Table.
- Click Add to create a new access entry.
- Select an entry in the Current Access Tables listbox and click Remove to delete the unwanted access entry.

MIBview Table

Configure the SNMPv3 MIB view table.

- **ViewName:** Type in a new view name in the field.
- **Sub-Oid Tree:** Type in the Sub OID that allows the view to access the objects of the level.
- **Type:** Select the radio button to determine the view type – exclude or included.
- Click Add to create a new entry.
- Click Remove to delete the unwanted entry.

QoS Configuration

You can configure **Qos mode**, **802.1p priority [7-0]** setting, **Static Port Ingress Priority** setting and **TOS** setting.

- **Qos Mode:** Click the pull-down menu to select the Qos policy rule.
  - **Disable QoS Priority:** The default status of Qos Priority is disabled.
  - **High Empty Then Low:** When all the high priority packets are empty in queue, low priority packets will be processed then.
  - **Highest:SecHigh:SecLow:Lowest:8:4:2:1:** The switch will follow the ratio of 8:4:2:1 to process priority queues including High, Middle, Low and Lowest. For example, while the system processing, 1 frame in the lowest queue, 2 frames in the low queue, 4 frames in the middle queue, and 8 frames in the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.
  - **Highest:SecHigh:SecLow:Lowest:15:7:3:1:** The process order is in compliance with the transfer rate of 15:7:3:1.
  - **Highest:SecHigh:SecLow:Lowest:15:10:5:1:** The process order is in compliance with the transfer rate of 15:10:5:1.
- **802.1p priority [7-0]:** Configure each priority level.
  - **Priority 0 ~ 7:** each priority has 4 priority levels – Highest, SecHigh, SecLow, and Lowest.
- **Static Port Ingress Priority:** The port ingress level is from 0 to 7.
- **TOS:** the system provides 0~63 TOS priority level. Each level has 8 priorities – 0~7. The default value is “0” priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example: user set the TOS level 25 is 0. The port 1 is following the TOS priority policy only. When the port 1 packet received, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25(priority = 0), and then the packet priority will have highest priority.
- When finished, click Apply.

Qos Configuration

Qos Mode: Disable QoS Priority

- Disable QoS Priority
- High Empty Then Low
- Highest:SecHigh:SecLow:Lowest = 8:4:2:1
- Highest:SecHigh:SecLow:Lowest = 15:7:3:1
- Highest:SecHigh:SecLow:Lowest = 15:10:5:1

802.1p Priority:

7	6					1	0
Lowset	Lowset	Low				set	Lowset

Default Ingress Port Priority Mapping:

Port.1-1	OFF	Port.2-1	OFF	Port.3-1	OFF	Port.4-1	OFF
Port.1-2	OFF	Port.2-2	OFF	Port.3-2	OFF	Port.4-2	OFF
Port.1-3	OFF	Port.2-3	OFF	Port.3-3	OFF		
Port.1-4	OFF	Port.2-4	OFF	Port.3-4	OFF		
Port.1-5	OFF	Port.2-5	OFF	Port.3-5	OFF		
Port.1-6	OFF	Port.2-6	OFF	Port.3-6	OFF		
Port.1-7	OFF	Port.2-7	OFF	Port.3-7	OFF		
Port.1-8	OFF	Port.2-8	OFF	Port.3-8	OFF		

TOS/DSCP Priority Mapping:

TOS1	0	TOS17	0	TOS33	0	TOS49	0
TOS2	0	TOS18	0	TOS34	0	TOS50	0
TOS3	0	TOS19	0	TOS35	0	TOS51	0
TOS4	0	TOS20	0	TOS36	0	TOS52	0
TOS5	0	TOS21	0	TOS37	0	TOS53	0
TOS6	0	TOS22	0	TOS38	0	TOS54	0
TOS7	0	TOS23	0	TOS39	0	TOS55	0
TOS8	0	TOS24	0	TOS40	0	TOS56	0
TOS9	0	TOS25	0	TOS41	0	TOS57	0
TOS10	0	TOS26	0	TOS42	0	TOS58	0
TOS11	0	TOS27	0	TOS43	0	TOS59	0
TOS12	0	TOS28	0	TOS44	0	TOS60	0
TOS13	0	TOS29	0	TOS45	0	TOS61	0
TOS14	0	TOS30	0	TOS46	0	TOS62	0
TOS15	0	TOS31	0	TOS47	0	TOS63	0
TOS16	0	TOS32	0	TOS48	0	TOS64	0

Apply Help

QoS Configuration interface

IGMP Configuration

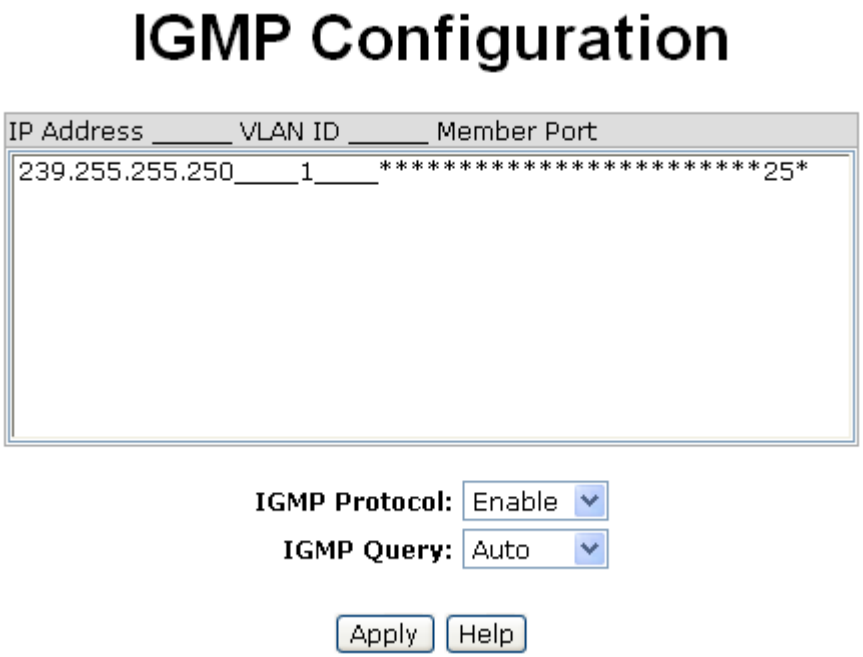
IGMP is the protocol used by IPv4 systems to report their IP multicast group memberships to neighboring multicast routers. IGMPv3 adds support for "source filtering", that is, the ability for a system to report interest in receiving packets only from specific source addresses, or from all but specific source addresses, sent to a particular multicast address.

IGMP have three fundamental types of message as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

With the switch supporting IP multicast, you can enable IGMP/MLD protocol via this interface. Destination IP multicast addresses range from 224.0.0.0 to 239.255.255.255.

- **IGMP Protocol:** Enable or disable the IGMP protocol.
- **IGMP Query:** Select the IGMP query function as Enable or Auto to set the switch as a querier for IGMP version 2 multicast network.
- Click Apply.



IGMP Configuration interface

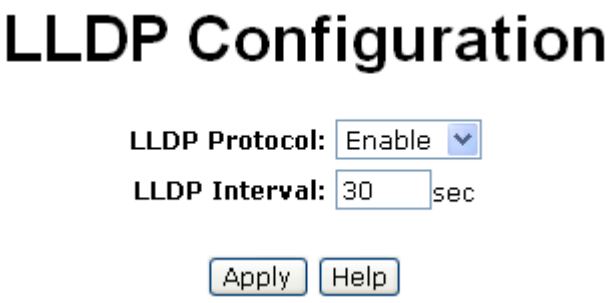
LLDP

Link Layer Discovery Protocol (LLDP), a one way protocol, specified in the IEEE 802.1AB standard allows stations attached to the same IEEE 802 LAN to advertise their information to neighbors and store the information received from adjacent stations.

Receivers on the same physical LAN will store the information distributed via LLDP in a standard Management Information Base (MIB) where the information can be accessed by a Network Management System (NMS) using a protocol like the Simple Network Management Protocol (SNMP).

LLDP runs on all 802 media. The protocol runs over the data-link layer only, allowing two systems running different network layer protocols to learn about each other.

- **LLDP Protocol**: Click the pull-down menu to disable or enable the LLDP function.
- **LLDP Interval**: Type the value in seconds as the interval for the switch to advertise its information to other nodes.
- Click Apply to have the configuration take effect.



LLDP Configuration interface

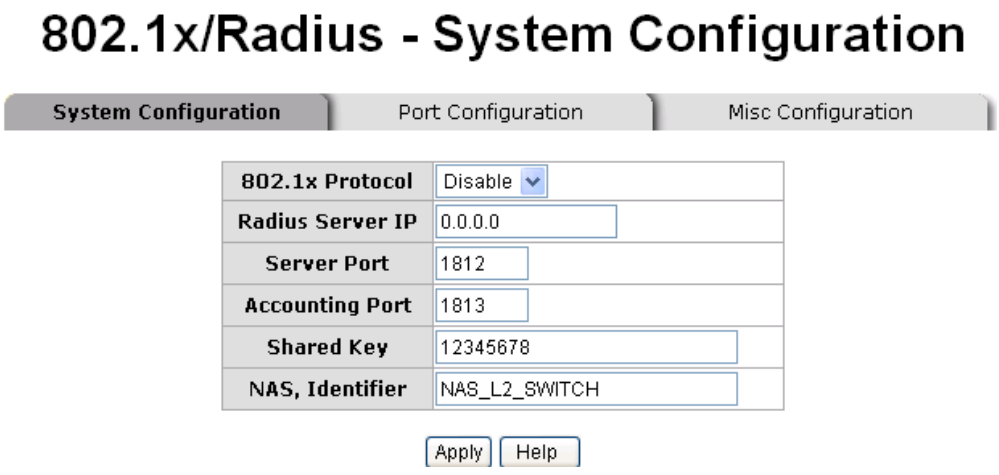
802.1x/Radius

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until it provides authority, like a user name and password that are verified by a separate server.

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

- **IEEE 802.1x Protocol:** .Enable or disable 802.1x protocol.
- **Radius Server IP:** Set the Radius Server IP address.
- **Server Port:** Set the UDP destination port for authentication requests to the specified Radius Server.
- **Accounting Port:** Set the UDP destination port for accounting requests to the specified Radius Server.
- **Shared Key:** Set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
- **NAS, Identifier:** Set the identifier for the radius client.
- Click the Apply button to have the configuration take effect.

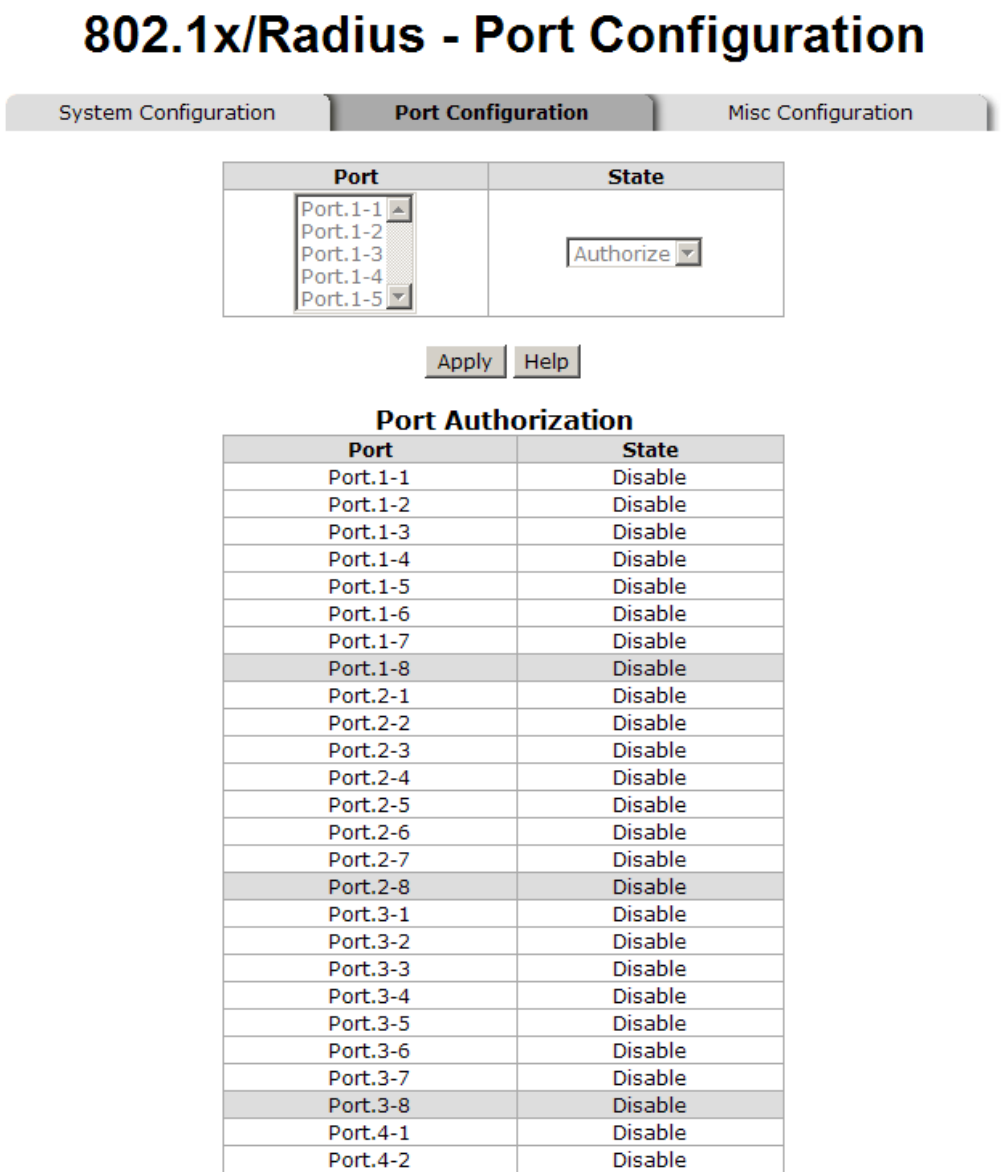


802.1x System Configuration interface

Port Configuration

You can configure 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize. Use "**Space**" key to change the state value.

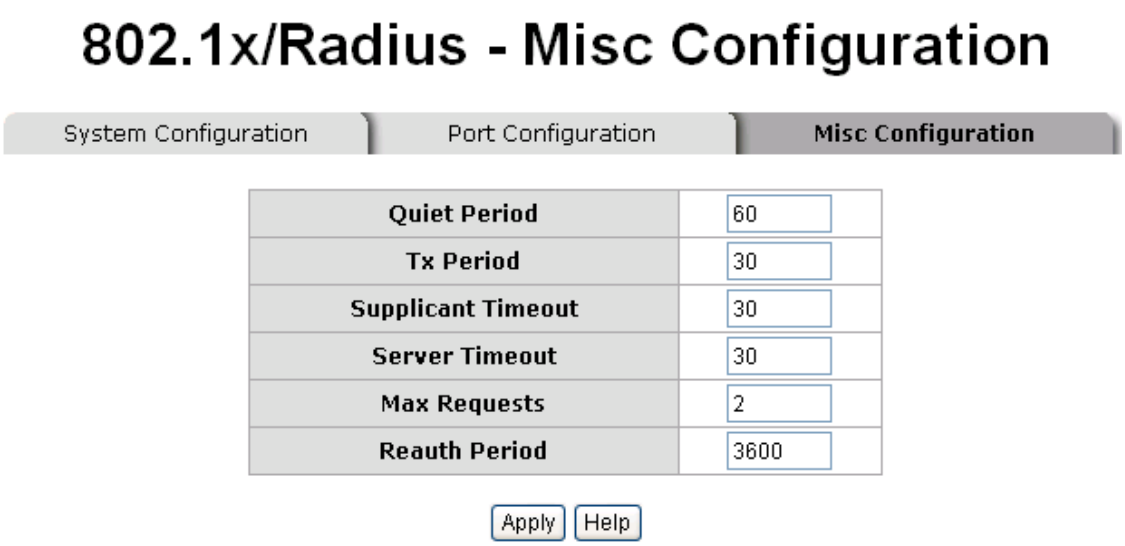
- **Reject:** The specified port is required to be held in the unauthorized state.
- **Accept:** The specified port is required to be held in the Authorized state.
- **Authorized:** The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the supplicant and the authentication server.
- **Disable:** The specified port is required to be held in the Authorized state
- Click Apply to have the configuration take effect.



802.1x Per Port Setting interface

Misc Configuration

- **Quiet Period:** Set the period during which the port doesn't try to acquire a supplicant.
- **TX Period:** Set the period the port waits for retransmitting the next EAPOL PDU during an authentication session.
- **Supplicant Timeout:** Set the period of time the switch waits for a supplicant response to an EAP request.
- **Server Timeout:** Set the period of time the switch waits for a server response to an authentication request.
- **Max Requests:** Set the number of authentication that must time-out before authentication fails and the authentication session ends.
- **Reauth period:** Set the period of time the connected clients authenticated to be authenticated again.
- Click Apply to have the configuration take effect.



802.1x Misc Configuration interface

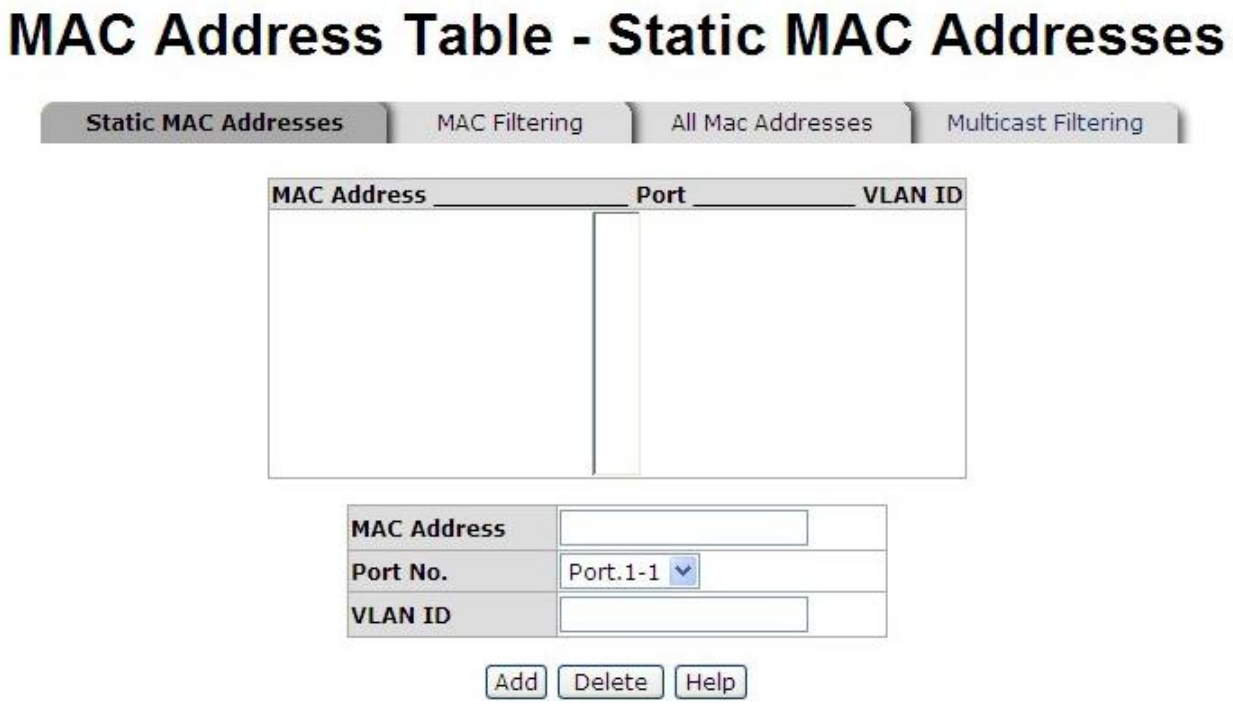
MAC Address Table

The MAC Address Table interface allows users to configure static MAC addresses, MAC filtering, multicast filtering and provides information of all MAC addresses on each port.

Static MAC Address

You can add a static MAC address that remains in the switch's address table regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a particular device's MAC address when the disconnected or powered-off device is active on the network again. Via this interface, you can add, modify and delete a static MAC address.

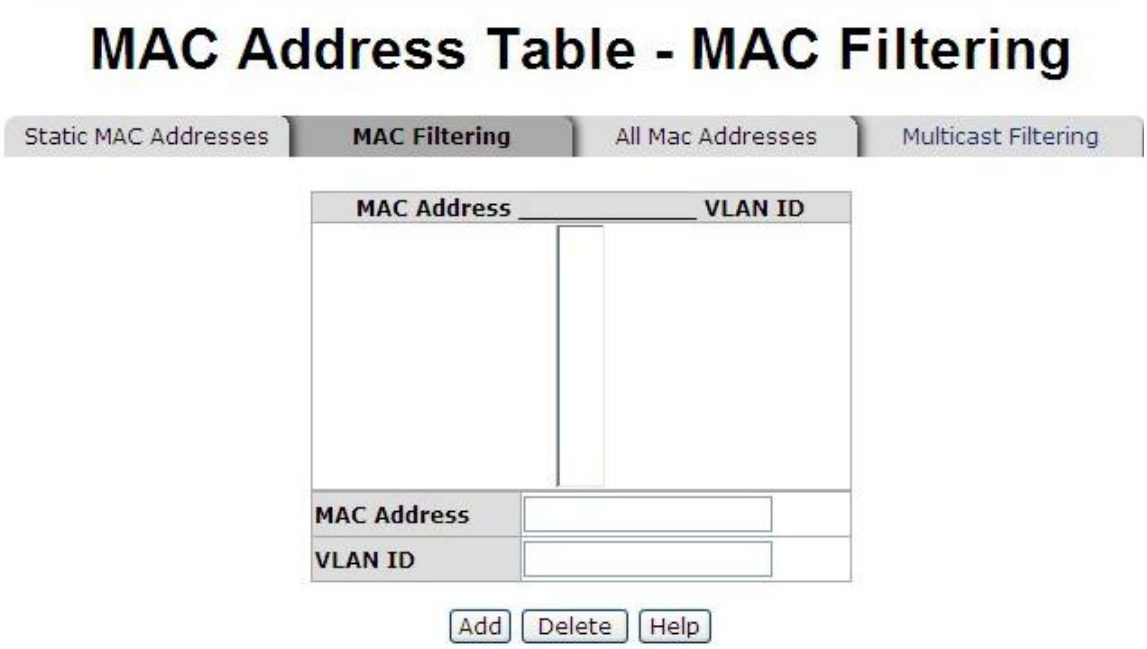
- **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
- **Port No.:** Click the pull-down menu to select the port number.
- **VLAN ID:** Type in VLAN group ID where the MAC address belongs.
- Click the Add button to finishing adding the entry.
- If you want to delete the entry from the table, select the MAC address entry listed in the table and click the Delete button.



Static MAC Addresses interface

MAC Filtering

By filtering MAC address, the switch can easily filter pre-configured MAC addresses and reduce the un-safety. You can add or delete filtering MAC addresses.

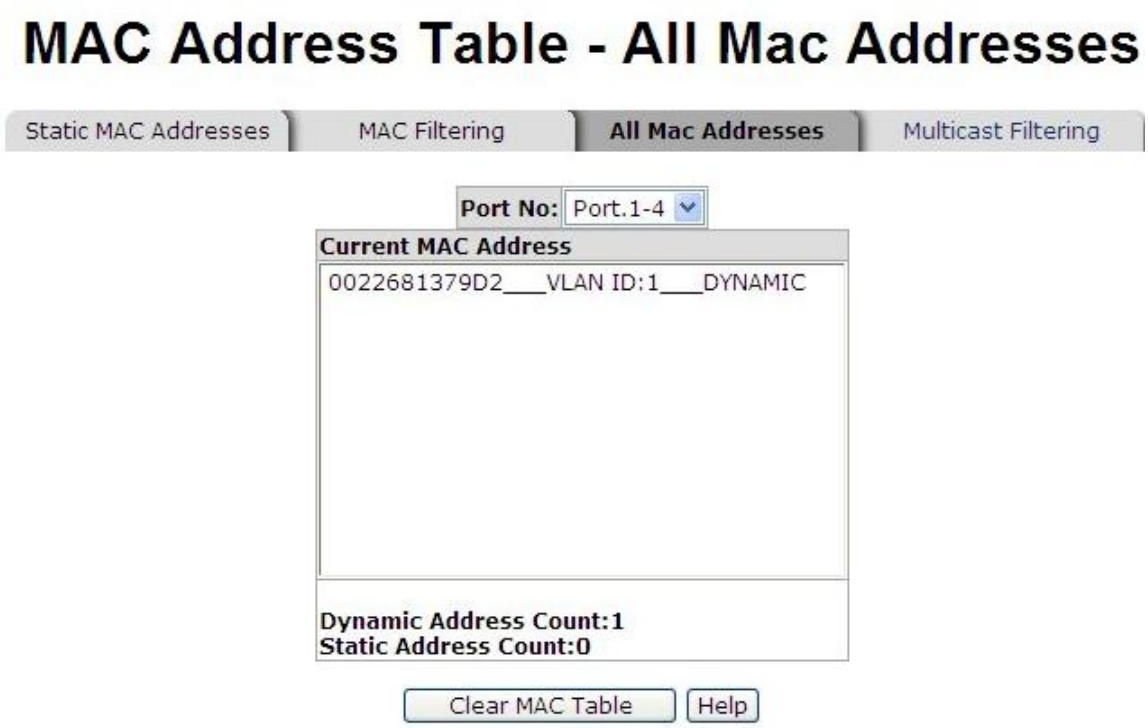


MAC Filtering interface

- **MAC Address:** Enter the MAC address to be filtered.
- **VLAN ID:** Type in the VLAN group ID the MAC address belongs.
- Click Add.
- If you want to delete the entry from the filtering table, select the MAC address entry listed in the table and click the Delete button.

All MAC Addresses

This tab displays all MAC address entries learned or set.



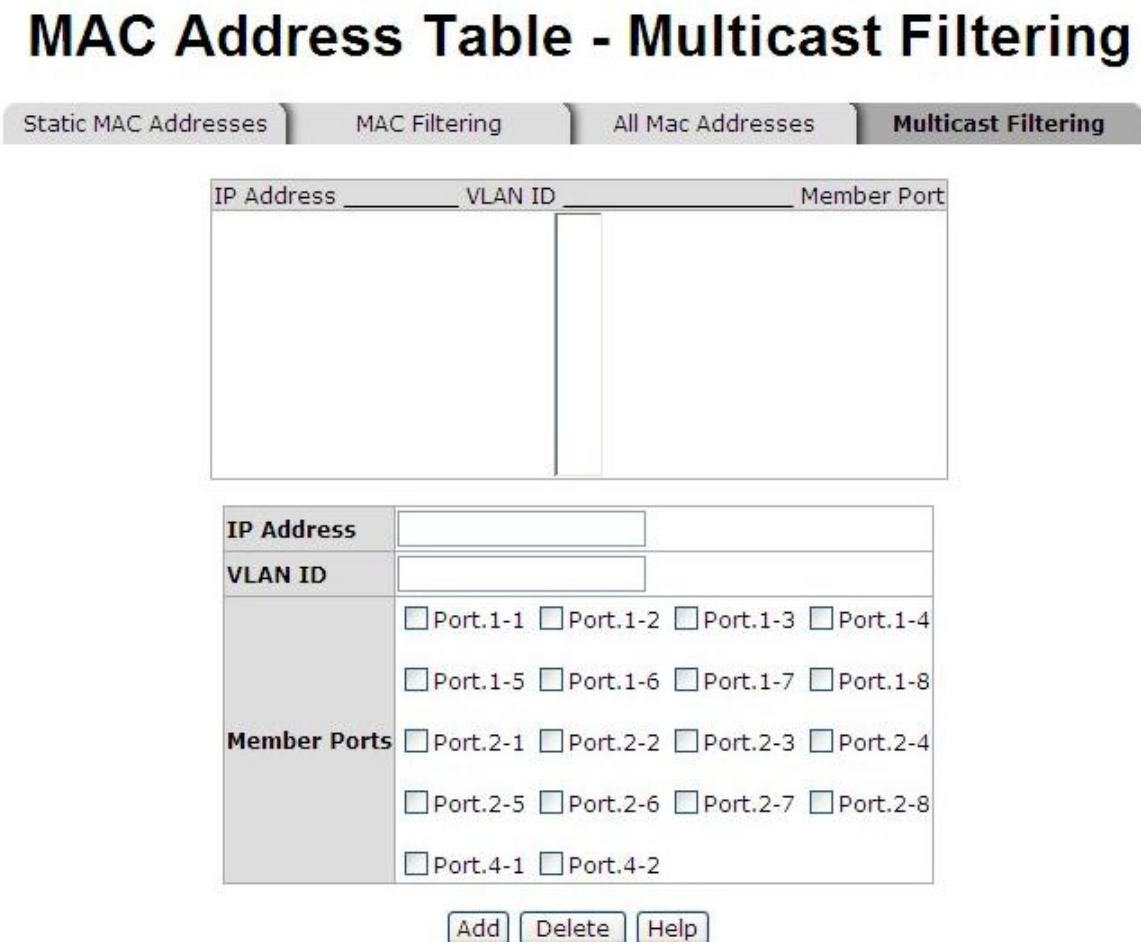
All MAC Address interface

- **Port No:** Click the pull-down menu to select a particular port to show its information.
- **Current MAC Address:** Information of the selected port will be displayed in this field.
- Click the Clear MAC Table button to clear the listed entries of the current static MAC address information.

Multicast Filtering

Similar to broadcasts, multicasts are sent to all end stations on a LAN or VLAN. Multicasting filtering is the function which end stations can receive the multicast traffic if the connected ports had been included in the specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations.

- **IP Address:** Assign a multicast group IP address in the range from 224.0.0.0 to 239.255.255.255.
- **VLAN ID:** Type in VLAN group ID where the MAC address belongs.
- **Member Ports:** Tick the checkbox in front of the port number to include the port as the member port in the specific multicast group of the given IP address.
- Click the Add button to finishing adding the entry.
- If you want to delete the entry from the table, select the entry listed in the table and click the Delete button.

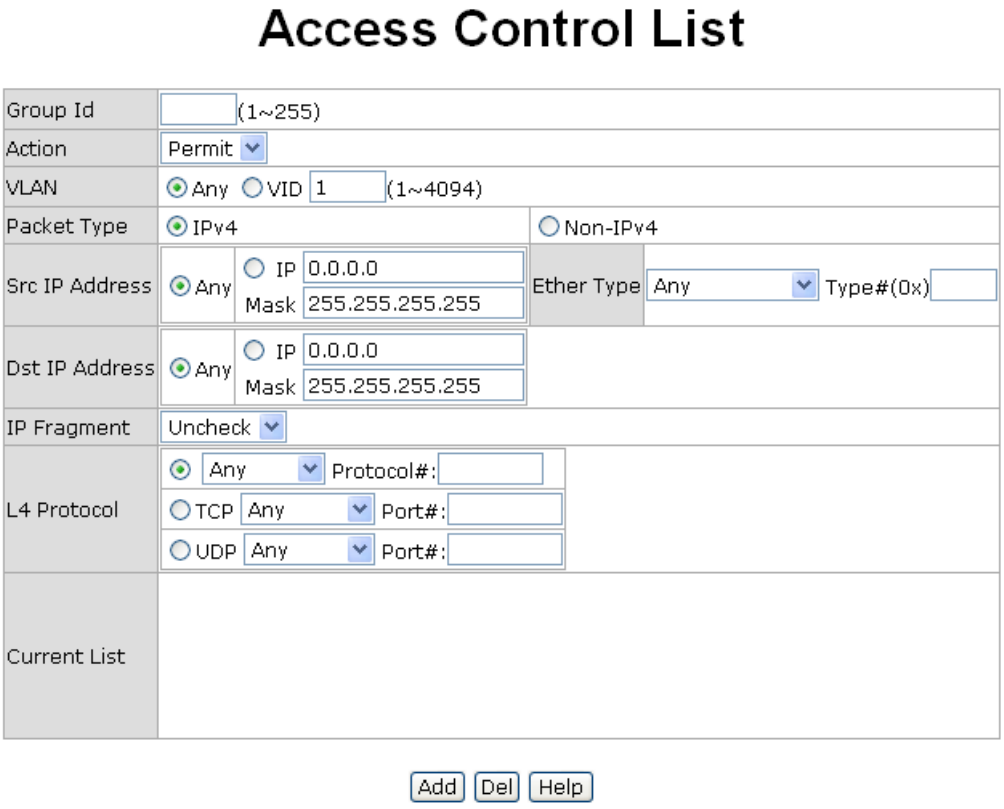


Multicast Filtering interface

Access Control List

The switch provides a 256-entry access control list (ACL) to check IPv4/non-IPv4 addresses and TCP/UDP port numbers of packets.

- **Group Id:** Type in the Group ID from 1 to 255 for the access control list being configured.
- **Action:** Click the pull-down menu to select *Permit* or *Deny* for the control list. *Permit* means traffic checked against this access control list will be processed. As for *Deny*, traffic will be dropped.
- **VLAN:** Select one of the radio buttons to determine packets entering any or a particular VLAN will be checked against this control list.
- **Packet Type:** Select the packet type—IPv4 or Non-IPv4
- **Src IP Address:** Select any or assign an IP address with Subnet Mask for source IP address.
- **Dst IP Address:** Select any or assign an IP address with Subnet Mask for destination IP address.
- **Ether Type:** Click the pull-down menu to select Any, ARP or IPX for Ether type.
- **IP Fragment:** Click the pull-down menu to determine whether the fragment is checked or not.
- **L4 Protocol:** Select the L4 protocol from among ICMP(1), IGMP(2), TCP or UDP.
- **Current List:** This field displays entries of the access control list.



Access Control List interface

Factory Default

Click the Reset button to reset the switch back to factory defaults. Before resetting, you can tick the checkboxes to keep the current IP address and user name/password.

Factory Default interface

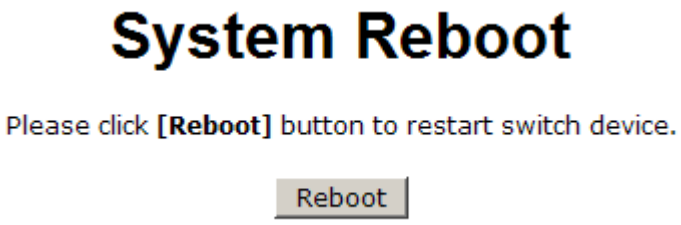
Save Configuration

Save all changes you have made in the system. To ensure the configurations you have made will be implemented the next time you power on the switch, remember to click the Save button to save the all configurations into the flash memory.

Save Configuration interface

System Reboot

Reboot the switch under software control. Click the Reboot button to restart the system.



System Reboot interface

6. Troubleshooting

This section is intended to help you solve the most common problems on the 3-slot intelligent chassis switch.

Incorrect Connections

The switch port can auto-detect straight or crossover cable when you link switch with other Ethernet devices. The RJ-45 connector should use correct UTP or STP cable; 10/100Mbps ports use 2-pair twisted cable and Gigabit 1000T ports use 4-pair twisted cable. Incorrect pin wiring will cause link failure. As for fiber connection, please notice that fiber cable mode and fiber module should match.

—Faulty or loose cables

Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. If that does not correct the problem, try a different cable.

—Non-standard cables

Non-standard and miss-wired cables may cause numerous network collisions and other network problem, and can seriously impair network performance. A category 5 cable tester is a recommended tool for every 100Base-T network installation.

—Improper Network Topologies

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, you should make sure that your network topology contains no data path loops. Between any two end nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

Diagnosing LED Indicators

The Switch can be easily monitored through panel indicators to assist in identifying problems, which describes common problems you may encounter and where you can find possible solutions.

IF the power indicator does turn on when the power cord is plugged in, you may have a problem with power outlet, or power cord. However, if the Switch powers off after running for a while check for loose power connections, power losses or surges at power outlet. IF you still cannot resolve the problem, contact your local dealer for assistance.

Cabling

RJ-45 ports: use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections, 100Ω Category 5 cable for 100Mbps or 100Ω Category 5e cable for 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet). The length does not exceed 100 meters.

7. Technical Specifications

This section provides the specifications of the 3-slot intelligent chassis switch as the table shown below.

Standard	IEEE802.3 10BASE-T IEEE802.3u 100BASE-TX/100BASE-FX IEEE802.3z Gigabit SX/LX IEE802.3ab Gigabit 1000T IEEE802.3x Flow Control and Back pressure IEEE802.3ad Port trunk with LACP IEEE802.1d Spanning tree protocol IEEE802.1w Rapid Spanning tree protocol IEEE802.1p Class of service IEEE802.1q VLAN Tagging IEEE802.1x User authentication
Switch Architecture	Store and forward switch architecture.
Back Plane	8.8Gbps
LED Indicators	System Power (Green) 8 10/100TX module: Link/Activity (Green), Full duplex/collision (Yellow) 8 100Base-FX module: Link (Green)/Activity (Green Blinking) 8 100SFP module: Link (Green)/Activity (Green Blinking) Gigabit Copper: Link/Activity (Green), 1000Mbps (Green), 100Mbps (Green), Full duplex/collision

	(Yellow) MINI GBIC: Link/Activity(Green), 1000Mbps (Green)
Connector	RS-232 console: 1 x DB-9 female 10/100TX module: 8 x RJ-45 100FX (Multi /Single Mode) module: 8 x SC 100SFP module: 8 x SFP Gigabit Copper + Mini-GBIC Combo: 2 x RJ-45 + 2 x Mini-GBIC
Expansion Module	■ 8 port 10/100TX module with RJ-45 connector ■ 8 port 100Mbps multi mode fiber module with SC connector ■ 8 port 100Mbps single mode fiber module with SC connector ■ 8 port 100Mbps SFP module
MAC Address	8K-entry
Packet Buffer	4Mbits
Flash ROM	4Mbytes
DRAM	16Mbytes
Jumbo Frame	9022bytes (only for Gigabit ports)
Power Consumption	50Watts (Maximum)
Dimensions	440mm (W) x 44mm (H) x 280mm (D)
Power Supply	100~240V_{AC}, 50 /60Hz, 0.8A (maximum)

	Redundant Power: DC 12 ~ 48V
Ventilation	2 x DC cooling fans with auto-detect function
Operating Temp.	-0℃~45℃, 5%~95%RH
Storage Temp.	-40℃~70℃, 5% ~ 95% RH
EMI	FCC Class A, CE
Safety	UL, cUL, CE/EN60950-1